NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

1st 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.

EC-CUBE's Cross-Site Scripting Vulnerabilities

In May 2021, EC-CUBE CO., LTD. revealed multiple cross-site scripting vulnerabilities. It has been confirmed that two of the vulnerabilities have already been exploited to make Stored XSS attacks. The attacker enters a malicious script in a data entry form on the EC site to store it in its database. When the administrator operates the administration screen, these vulnerabilities can be exploited to execute the malicious script. As a result, the attacker may steal authentication information, install a WebShell with which they can operate remotely and steal credit card information. NTT DATA proposes that administrators and developers of EC sites using EC-CUBE apply update programs and check for attacks and damage immediately.

Attacks against Mercari's Software Supply Chain

Mercari, Inc., which operates the flea market application "Mercari, "revealed in May 2021 that a third party had gained unauthorized access to its website, resulting in leakage of the company's customer information and other data to an external environment. One of the distinctive feature of the incident is that the attacker attacked Mercari's software supply chain and invaded its multiple systems in stages. This document explains how the attacker managed to invade the systems and what countermeasures should be taken to prevent such invasion into development environments.

Data Breach

Net Marketing Co. Ltd. revealed that fraudulent access was gained to the server that managed Omiai, a matchmaking application helping its users find a boyfriend/girlfriend and future husband/wife. Information about up to 1,711,756 users leaked, including image data of their driver's licenses, health insurance cards, passports and Individual Number Cards. This document explains the social impact of leakage of massive ID image data from the perspective of the reliability of an identity verification method using eKYC.

Outlook

There is a growing trend among countries affected by cyberattacks to name and criticize the countries involved in the attacker groups and their crimes. It is believed that such a trend will encourage state-sponsored attacker groups to further hide their identity information in order to prevent the involved countries from being exposed.

There is also the possibility that the cyberattacks coincided with the spread of the coronavirus. If COVID-19 worsens again and vaccine booster shots are required, there will be phishing attacks that exploit vaccination information. However, if we move on to the post-COVID world in the current state, it is predicted that there will be attacks on the pharmaceutical and healthcare industries, leisure-related phishing attacks, attacks targeting new businesses and investments and attacks on other wealthy industries in the post-COVID world.

2. Featured Topics

2.1. EC-CUBE's Cross-Site Scripting Vulnerabilities

On April 28, 2021 (U.S. time), Trend Micro released a blog about "Water Pamola," which was an attack campaign targeting online shops by placing fraudulent orders [1]. The company had been following the attack campaign named "Water Pamola" since 2019. Originally, Water Pamola penetrated online shops in Japan, Australia and European countries via spam mails containing malicious attachments. At the beginning of 2020, however, Water Pamola changed its attack approach and has been making cross-site scripting attacks ever since by using malicious scripts, rather than spam mails, as shown in Figure1. The victims of the malicious scripts are mainly in Japan. Therefore, it can be surmised that Water Pamola is targeting online shops in Japan.

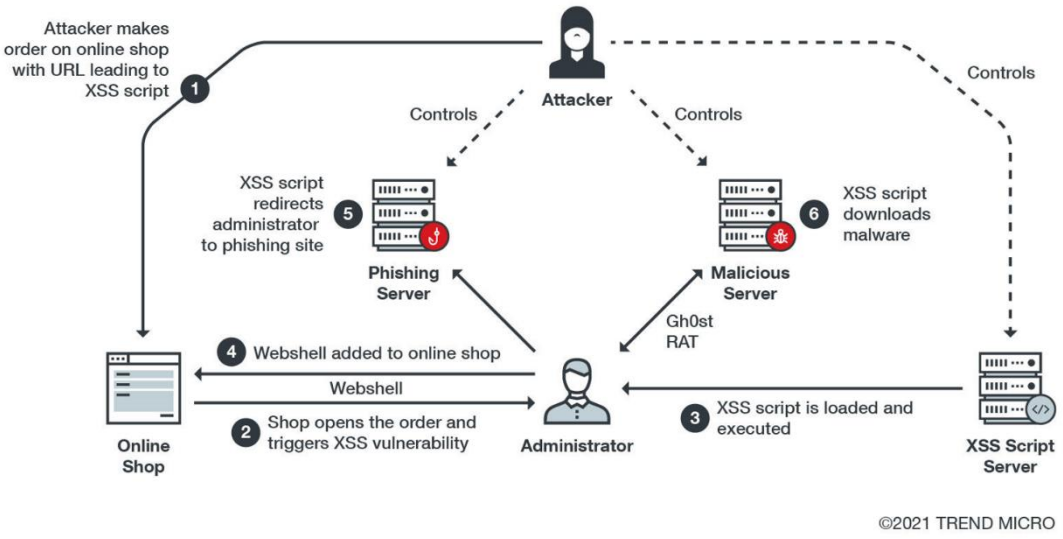


Figure1: Flow of Water Pamola Attack [1]

The results of an investigation conducted on an invaded EC site in 2021 found 35 credit card data breaches caused by unauthorized access. Figure2 shows the EC platforms used for the 35 breaches. It is predicted that the attacker may target EC-CUBE, which is used to build many EC sites.

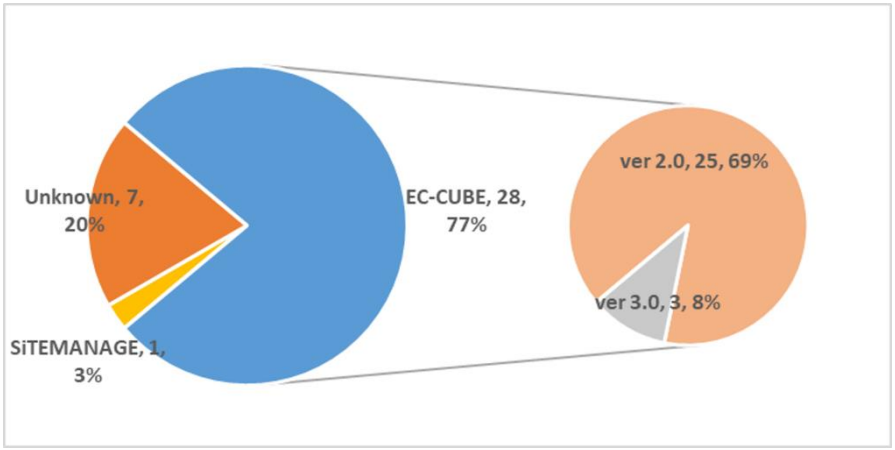


Figure2: Names and Versions of Penetrated EC Site Platforms

This document describes the new vulnerabilities of EC-CUBE that have been revealed since May 2021 to provide details of the vulnerabilities of EC-CUBE and the attack methods that exploit its vulnerabilities. The document also proposes security countermeasures that should be taken by EC site administrators using EC-CUBE.

2.1.1. Vulnerabilities of EC-CUBE

(1) Vulnerabilities of the main unit of EC-CUBE

Regarding EC-CUBE's cross-site scripting vulnerability (CVE-2021-20717) [3], EC-CUBE CO.,LTD. released an awareness raising article on May 7, 2021 [4]. Then, JPCERT/CC also released an awareness raising article on the same vulnerability on May 10 [5]. Information about the vulnerability is summarized in Table1.

The attacker exploits the vulnerability to enter a malicious script in a certain data entry field. When the administrator of the EC site operates a certain administration screen, the malicious script entered by the attacker is executed. If the malicious script is executed, the attack is successful and the attacker may gain unauthorized access to the EC site and steal credit card information. EC-CUBE CO.,LTD. confirms that there have already been several attacks exploiting the vulnerability.

Table1: Information about Vulnerability (CVE-2021-20717) [6]

Date published	May 7, 2021
CVE number	CVE-2021-20717
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	EC-CUBE 4.0.0 to 4.0.5
Vulnerability type	Cross-site scripting (Stored XSS)

On June 10, 2021, EC-CUBE CO.,LTD. published EC-CUBE's cross-site scripting vulnerabilities (CVE-2021-20750 and CVE-2021-20751) [7] [8]. Information about the vulnerabilities is summarized in Table2 and Table3.

Both CVE-2021-20750 and CVE-2021-20751 are vulnerabilities to Reflected XSS. The attacker directs the administrator or a user of the EC site to a fake site and makes them perform a certain operation. If the administrator or a user of a vulnerable site that uses EC-CUBE performs a certain operation on the site, a malicious script is executed on the administrator or user's web browser. If the attack is successful, the attacker may steal cookies from the user's browser and collect their credit card information or authentication information by means of a data entry form using HTML tags.

Table2: Information about Vulnerability (CVE-2021-20750) [9]

Date published	June 10, 2021
CVE number	CVE-2021-20750
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	・EC-CUBE 3.0.0 to 3.0.18-p2 ・EC-CUBE 4.0.0 to 4.0.5-p1
Vulnerability type	Cross-site scripting (Reflected XSS)

Table3: Information about Vulnerability (CVE-2021-20751) [9]

Date published	June 10, 2021
CVE number	CVE-2021-20751
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	EC-CUBE 4.0.0 to 4.0.5-p1
Vulnerability type	Cross-site scripting (Reflected XSS)

(2) Vulnerabilities of EC-CUBE plugins

On June 15, 2021, JPCERT/CC released awareness raising articles on cross-site scripting vulnerabilities of several plugins for EC-CUBE 3.0 [10]. Information about the vulnerabilities is summarized in Table4, Table5, Table6 and Table7.

Both CVE-2021-20735 and CVE-2021-20742 are vulnerabilities to Stored XSS. When these vulnerabilities are exploited, the attacker enters a malicious script in a data entry field on the EC-CUBE order screen, instead of order information, and then the entered script is stored in EC-CUBE's order database. When the administrator of EC-CUBE operates the administration screen for a certain EC-CUBE plugin such as the delivery slip No. plugin, the

malicious script is read from the order database, along with the order information, and processed on the administrator's web browser. Then, the malicious script is executed. JPCERT/CC has already detected some attacks exploiting CVE-2021-20735.

Table4: Information about Vulnerability (CVE-2021-20735) [11]

Date published	June 15, 2021
CVE number	CVE-2021-20735
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	・Delivery slip No. plugin (3.0) 1.0.10 and earlier versions ・Delivery slip No. csv batch registration plugin (3.0) 1.0.8 and earlier versions ・Delivery slip No. email plugin (3.0) 1.0.8 and earlier versions
Vulnerability type	Cross-site scripting (Stored XSS)

Table5: Information about Vulnerability (CVE-2021-20742) [12]

Date published	June 15, 2021
CVE number	CVE-2021-20742
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	・Plugin for EC-CUBE 3.0 "Form output plugin" Versions before 1.0.1 (Environments in EC-CUBE 3.0.0 to 3.0.8 only)
Vulnerability type	Cross-site scripting (Stored XSS)

On the other hand, CVE-2021-20743 and CVE-2021-20744 are vulnerabilities to Reflected XSS. The attacker prepares a modified page in advance, directs a user or the administrator to the page and makes them execute a certain operation. Then, a malicious script is executed on the browser of the user or administrator who used this certain vulnerable EC-CUBE plugin. If the attack is successful, they may access a phishing site or download a malicious program from a fake site and infect their company's environment.

Table6: Information about Vulnerability (CVE-2021-20743) [12]

Date published	June 15, 2021
CVE number	CVE-2021-20743
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	・Plugin for EC-CUBE 3.0 “Newsletter management plugin” Versions before 1.0.4 (Environments in EC-CUBE 3.0.0 to 3.0.8 only)
Vulnerability type	Cross-site scripting (Reflected XSS)

Table7: Information about Vulnerability (CVE-2021-20744) [12]

Date published	June 15, 2021
CVE number	CVE-2021-20744
CVSS score	6.1
CVSS metrics	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected products	・Plugin for EC-CUBE 3.0 “Category content plugin” Versions before 1.0.1 (Environments in EC-CUBE 3.0.0 to 3.0.8 only)
Vulnerability type	Cross-site scripting (Reflected XSS)

2.1.2. Reflected XSS and Stored XSS

The several EC-CUBE vulnerabilities described in 2.1.1 are divided into two types of cross-site scripting vulnerabilities: Reflected XSS and Stored XSS. Each type has its own attack methods. This section describes Reflected XSS and Stored XSS.

As shown in Figure3, vulnerabilities to cross-site scripting (XSS) can be classified into three types: Reflected XSS, Stored XSS and DOM Based XSS.

Figure3: XSS Types [13]

In typical Reflected XSS, the attacker prepares a fake site. First, the attacker sets up a fake site containing a malicious script. Then, the attacker sends the target user an email containing a URL to the fake site and directs the user to the fake site. When the user accesses the fake site, the malicious script is sent to the user as its response and executed on the user's web browser. The executed malicious script steals cookie information and authentication information from the browser.

In Stored XSS, on the other hand, the attacker sends a character string containing a malicious script to a web server, as shown in Figure4. Then, the character string is stored in the web server or its database. When the user accesses the website, the character string stored in the web server or database is output. As a vulnerability exists in the character string output/display process, the character string is executed on the browser as a malicious script. This malicious script downloads malware, etc. and executes it on the user's device.

If the user notices a phishing email or other data received from the attacker and does not follow its guidance, Reflected XSS does not cause any concern such as clicking on a suspicious URL and receiving a Reflected XSS attack. In Stored XSS, on the other hand, there is no suspicious event such as a phishing email. When the user simply displays website information as usual, the malicious script is automatically executed on the user's browser. It is believed that since Stored XSS is a more concealed attack method involving no screen transitions on the web browser, it is more difficult to detect the execution of a malicious script and its damage can spread more easily.

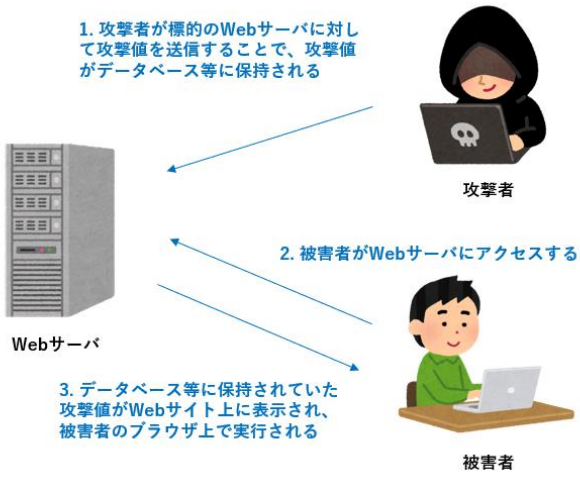


Figure4:　Stored XSS Attack Flow　[14]

2.1.3. Explanation of Example of Attack Exploiting EC-CUBE Vulnerabilities

As described in 2.1, Trend Micro detected an attack activity by Water Pamola, which made a cross-site scripting attack on the EC site. JPCERT/CC also confirmed similar attacks. On July 6, 2021, JPCERT/CC released a blog post that explained attacks exploiting EC-CUBE vulnerabilities (CVE-2021-20717 and CVE-2021-20735)　[15]. The flow of an XSS attack on EC-CUBE vulnerabilities (CVE-2021-20717 and CVE-2021-20735) is shown in Figure5.

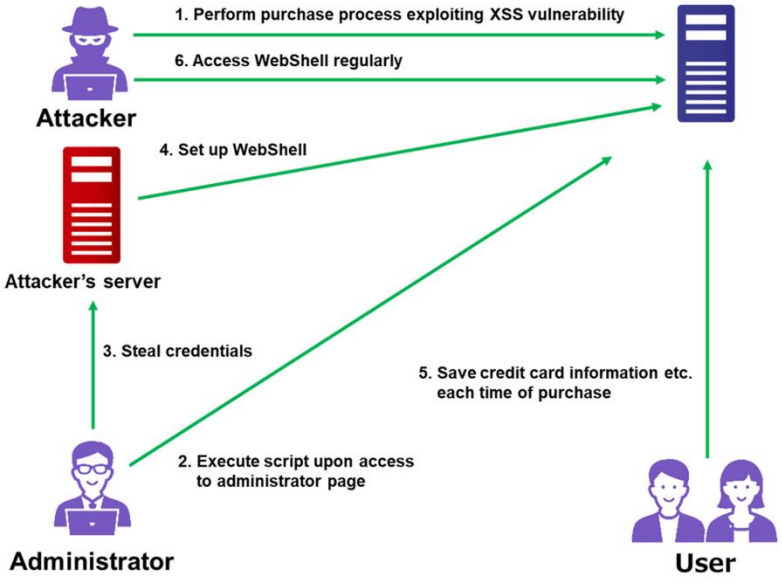


Figure5: Flow of XSS Attack　[15]

The attacker enters a character string containing a malicious script, as shown in Figure6, in an order form on the EC site that was created using EC-CUBE, which has vulnerabilities, and then executes the purchasing process (① in Figure5). Normally, even if a character string contains a malicious script, sanitization is performed to prevent the script from being executed unintentionally. On a site using EC-CUBE 4.0, where CVE-2021-20717 exists, the sanitization is disabled. As a result, the character string containing the malicious script is stored in EC-CUBE's database as is.

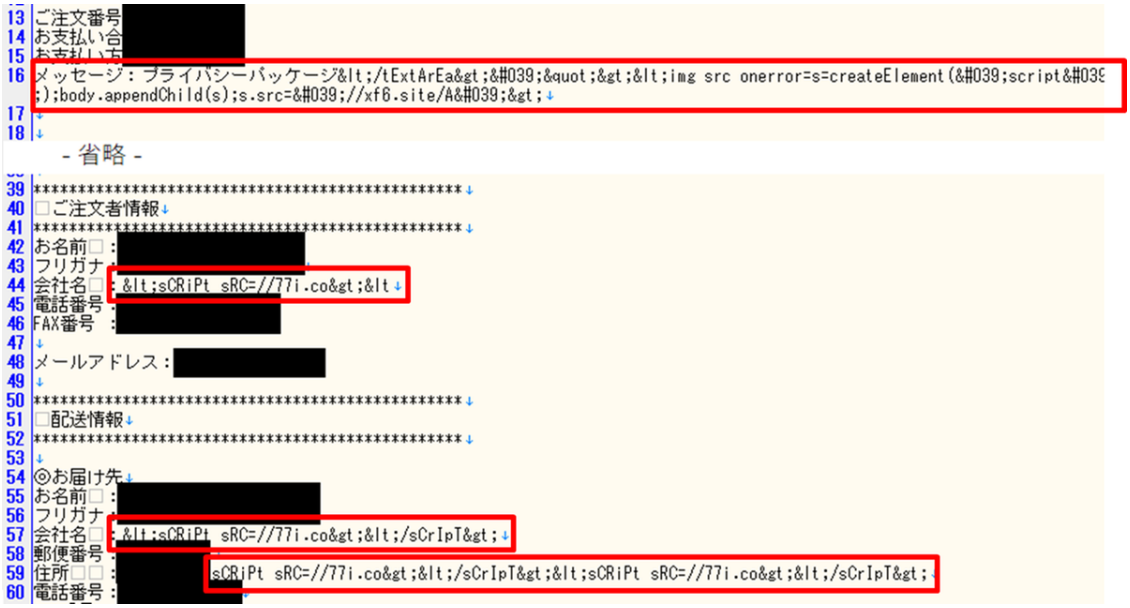


Figure6: Order Details Targeting XSS in Multiple Data Entry Fields [15]

Next, the administrator of the EC site accesses the administration screen for EC-CUBE and displays details of the order (② in Figure5). Then, the character string containing the malicious script is read from EC-CUBE's database and displayed as a script on the administration screen.

This vulnerability may also exist in a site using a plugin for EC-CUBE 3.0 where sanitization is implemented. As the html_entity_decode function is used in certain plugins for EC-CUBE 3.0, the character string converted through sanitization is changed back to the original malicious character string that can be executed as a script, and then output to the web browser. When the EC site administrator views the order on the administration screen as usual, using the corresponding plugin feature, the malicious script is executed on the administrator's device. The attacker's malicious script steals the authentication information of the administrator and sends it to the attacker's administration server. Then, the attacker uses the stolen authentication information to log in to the EC site and install a WebShell (③ and ④ in Figure5). The attacker operates the EC site via the installed WebShell remotely

and steals credit card information, as shown in Figure7, until the WebShell is found and removed. (⑤ and ⑥ in Figure5)

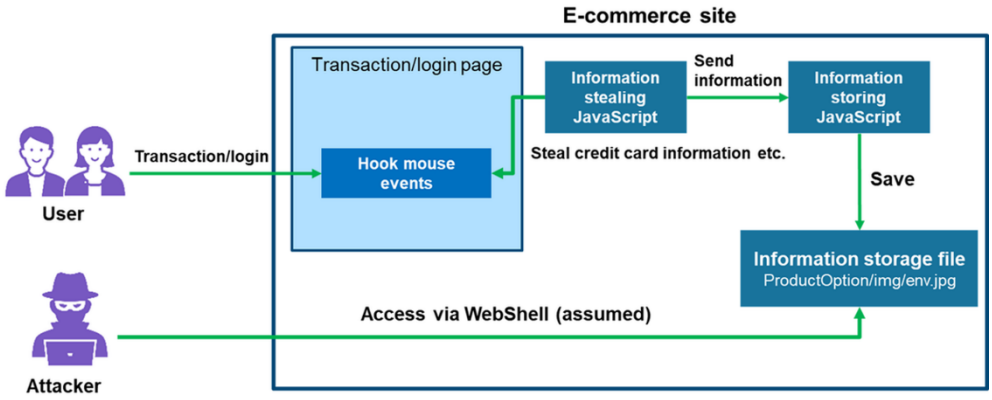


Figure7: Flow of Stealing Credit Card Information, etc. [15]

2.1.4. Proposals for Security Countermeasures to Administrators of EC-CUBE Sites

Check your version of EC-CUBE according to the version check procedure [16] provided by EC-CUBE CO.,LTD. and fix the vulnerabilities of the applicable version as described in (1) below. If you are using a product of any vulnerable version, be sure to perform (2) Checking for attacks and (3) Checking for damage as well.

(1) Checking your version and fixing its vulnerabilities

1 If you use EC-CUBE4.0,

Update EC-CUBE4.0 to the latest version, “EC-CUBE 4.0.6-p1” [17]. If you customized the source code for the main unit of EC-CUBE, reflect the fixing difference in the code.

Once it is updated to the latest version, CVE-2021-20750 and CVE-2021-20751 will be fixed, including CVE-2021-20717. For a detailed fixing method, refer to the vulnerability page [8], which was released by EC-CUBE CO.,LTD.

2 If you use EC-CUBE 3.0,

(a) Fixing vulnerabilities of the main unit of EC-CUBE 3.0

Apply the fixing patches for EC-CUBE 3.0. If you customized the source code for the main unit of EC-CUBE, reflect the fixing difference in the code.

For a detailed fixing method, refer to the vulnerability page [7], which was released by EC-CUBE CO.,LTD.

(b) If you use an ETUNA plugin related to delivery slip No.

There have already been some attacks exploiting the vulnerabilities. If you use

any of the affected plugins listed in Table8, update it to the latest version immediately.

Table8: How to Update ETUNA Plugins

Affected plugin	Updating method
Delivery slip No. plugin (3.0)	Update it to 1.0.11 or a later version [18].
Delivery slip No. csv batch registration plugin (3.0)	Update it to 1.0.9 or a later version [19].
Delivery slip No. email plugin (3.0)	Update it to 1.0.9 or a later version [20].

(c) If you use an EC-CUBE plugin

There have already been some attacks exploiting the vulnerabilities. If you use any of the affected plugins listed in Table9, update it to the latest version immediately.

Table9: How to Update EC-CUBE Plugins

Affected plugin	Updating method
Form output plugin	Update it to 1.0.1 or a later version [21].
Newsletter management plugin	Update it to 1.0.4 or a later version [22].
Category content plugin	Update it to 1.0.1 or a later version [23].

(d) If you develop a plugin for EC-CUBE

EC-CUBE CO.,LTD. provides a sample plugin called “category content plugin” to developers of plugins for EC-CUBE 3.0 [24]. Since the plugin uses the http_entity_code function, cross-site scripting attacks may be launched by converting sanitized data back into an executable script and outputting it, as described in 2.1.3. Check if the developed plugin uses the html_entity_decode function. If it does, refer to the EC-CUBE fixing method [25] to fix the source code.

The latest version of the category content plugin (1.0.1) was released on June 14, 2021 [26]. If an old version was used to develop a plugin in the past and EC-CUBE 3.0.0 to 3.0.8 is currently used, there may be some impact.

(2) Checking for attacks

These vulnerabilities exist in all versions of EC-CUBE 3.0 series and 4.0. series. Several plugins that are used frequently also contain vulnerabilities. As attackers actively attacked online shops that had these vulnerabilities in Japan, some of them are likely to have already been attacked. After fixing the vulnerabilities, be sure to check whether there has been an attack. If you receive a Stored XSS attack that exploits a vulnerability such as CVE-2021-20717, the attacker has entered ”<script>”, which is a character string that can be converted into a script, into a data entry field such as a name, address or company name of databases related to a customer, order or delivery, and then stored it. In that case, “<” and “>” have been sanitized and replaced by character strings of “<” and “>”. Search the database for the character string “<script>”. If an investigation is made via the administration screen, an attempted attack may be executed. Therefore, search the database directly or investigate the bodies of the order emails remaining in the Mail Box.

(3) Checking for damage

If any sign of an attack is detected, separate the EC-CUBE system from the network immediately and contact the security manager quickly. JPCERT/CC releases the IPs and domains of attackers or the SHA256 hash values of the files used for attacks [5]. Use the information to investigate details of any damage caused by the attacker. If a WebShell is installed on the EC site or any sign of communication from the EC site to a suspicious IP address or domain is detected, it is likely that credit card information has been stolen or other damage has been caused. Handle the incident by notifying the affected customers of fraudulent use of their credit cards, reporting the incident to information security organizations or authorities, and so forth.

2.1.5. Conclusion

This section described the new vulnerabilities of EC-CUBE that were revealed in 2021 and attack methods exploiting the vulnerabilities. Of the revealed vulnerabilities of EC-CUBE, CVE-2021-20717 and CVE-2021-20717, which are vulnerabilities to Stored XSS, have been exploited to make attacks. Administrators of EC sites using EC-CUBE are requested to check their version immediately.

EC-CUBE is easily targeted by attackers and attack campaign of the Water Pamola is also targeting vulnerabilities of EC-CUBE in Japan. If you are using a vulnerable version in which an attack has been made before, you may have already received an attack. If you detect an attack or any sign of damage, block the network of the EC site and notify your customers immediately to minimize its damage.

2.2. Attacks against Mercari's Software Supply Chain

2.2.1. Overview of the Incident

Mercari, Inc. (hereinafter "Mercari"), which operates the flea market application "Mercari," revealed in May 2021 that a third party had made unauthorized access to its website, resulting in leakage of the company's customer information and other data to an external environment [27]. One of the characteristics of this incident is that the attack targeted a software supply chain by making unauthorized access to a third-party code coverage tool called "Codecov" as its springboard. This section explains how the attacker managed to invade several systems and what countermeasures should be taken to prevent such invasion.

2.2.2. Three-Step Attack on Software Supply Chain

(1) Mercari's system development environment

First, this section describes the system environment where the incident occurred. Mercari's systems were developed in a continuous integration environment (CI environment) shown in Figure 8). Codecov and other code coverage tools visualize how much the testing of a source code that is being developed is completed. It is believed that in Mercari's system development environment, Codecov was used to test applications that were being developed in the CI environment and their tested source codes were stored in GitHub. It is also surmised that the production environment was isolated from the CI environment in terms of the network.

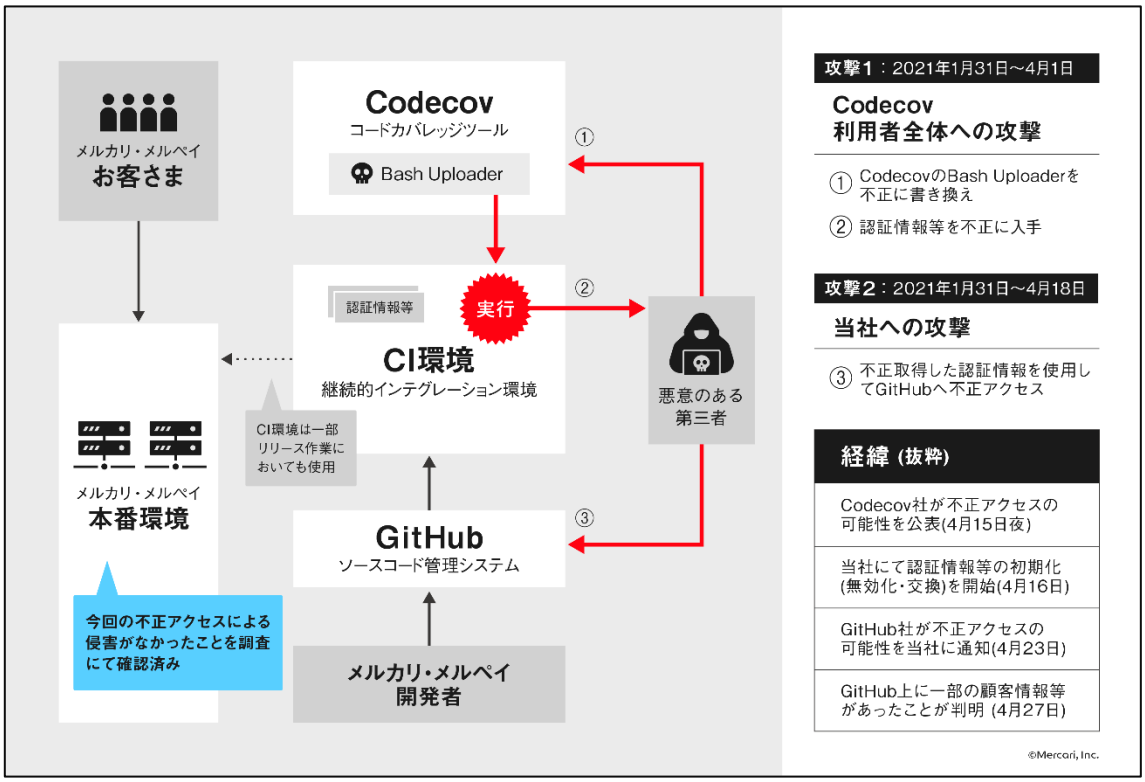


Figure 8: Mercari's System Development Environment [27]

(2) Explanation of the three-step attack on the software supply chain

This section describes the attacks made during the incident, based on the information released by Mercari and Codecov.

1 Attack on Codecov

The attacker exploited an error in the process of creating Docker images on the Codecov system and stole authentication information about the authority to rewrite the Codecov Bash Uploader script. After January 31, 2021 (U.S. time), the attacker used the stolen authentication information to falsify the Codecov Bash Uploaderscript [28]. The Bash Uploader script is used by Codecov customers to send reports on test results (code coverage reports) to the Codecov platform. Once a report is sent to the Codecov platform, test results can be merged and analyzed results can be obtained.

2 Obtaining information from the CI environment

The falsified Bash Uploaderscript was modified so as to obtain and send authentication information about Codecov users to the attacker. When Mercari's developer downloaded the falsified Bash Uploader script to Mercari's CI environment and executed it in order to send a code coverage report, the authentication information and other data that the developer was using in the CI environment was sent to the attacker. As the leaked information contained the authentication information that

Mercari used to log in to GitHub, the range of the attacker's invasion reached as far as the GitHub environment.

3 Attack on Github

On April 22, GitHub detected suspicious activity related to Codecov. On April 23, the company notified Mercari that some of the source codes stored in GitHub might have been affected by the falsified Bash Uploader script. In response, Mercari investigated its repository logs on GitHub and discovered that GitHub had received unauthorized access. The repository stored the source codes that constituted Mercari's applications, and the source codes contained customer information and other data. The attacker stole the source codes stored in the repository, and information about 27,927 customers in total leaked. (This includes the additional information released on August 6, 2021 [29].)

(3) Impact of the incident

According to the results of an investigation conducted by Mercari, some of the information that leaked from GitHub is as shown below. What should be noted is that the leaked information was quite old.

1. Some of the source codes for Mercari (including the U.S. version of Mercari and services provided in the past) and Merpay that were stored in GitHub
2. Account transfer data and inquiry data of Mercari's customers that was contained in the above source codes (including personal information)
   - Information about money transfers of proceeds into customers' accounts that were executed between August 5, 2013 and January 20, 2014 (bank code, branch code, account number, account holder (in kana), transferred amount): 17,085 cases
   - Information about customer service responses between November 2015 and January 2018 (name, address, email address, phone number, inquiry details): 217 cases
   - Information about events held in May 2013 (name, age, gender, email address): 6 cases
   - Information about customer service responses between December 2015 and February 2019 (name, address, birthday, transaction message): 13 cases (additional information released on August 6, 2021 [29])
3. Information about some partners of Mercari and Merpay that was contained in the above source codes:
   - Merpay partner information (names of individual owner-managers): 7,925 cases
   - Information about partners of Mercari and Merpay (name, birthday, organization, email address, etc.): 41 cases
   - Personal information of some employees of Mercari, Inc. (including its subsidiaries) (names, company email addresses, employee ID, phone numbers,

birthdays and other information about some employees as of April 2021; *including past employees and some external subcontractors): 2,615 cases

- Personal information of some employees of Mercari, Inc. (including its subsidiaries) (names, company email addresses, employee ID and other information about some employees as of April 2021; *including past employees and some external subcontractors): 25 cases (additional information released on August 6, 2021 [29])

The information leaked in the incident contained very old information such as “Information about money transfers of proceeds into customers’ accounts that were executed between August 5, 2013 and January 20, 2014.” According to Mercari’s policy, customer information should not be stored in GitHub. In the past, however, there were some operational breaches [30]. As indicated above, storing confidential information that is not required for the operation in a system incurs the risk of information breaches, when unauthorized access is made.

2.2.3. Attacker’s aim

In this incident, the attacker attacked a third-party product in use as a springboard to steal authentication information from GitHub. As a result, customers’ personal information, account information and other data leaked from GitHub.

However, was the attacker’s original aim really to steal the personal information stored in GitHub? Although this is pure supposition, the attacker probably didn’t aim to steal massive personal information from GitHub since massive personal or account information generally are not stored in GitHub, and Mercari, Inc. also has a rule that stipulates that personal information and authentication information should not be stored in GitHub. It is surmised that as shown in the example of the attack on “EC-CUBE” described in Past Quarterly Report on Global Security Trends (1st Quarter of 2019 [31]), the attacker’s original aim was to steal credit card information by entering the production environment of an EC-related system, falsifying a front-end online site and embedding a malicious program into it.

Fortunately, the Mercari incident did not result in any damage such as invasion of the production environment by the attacker or impact of the falsified program on the service in operation [27] [32]. While how Mercari, Inc. prevented the attack is unknown, the next section explains what countermeasures should be taken in response to software supply chain attacks like this incident.

2.2.4. Countermeasures

In the SolarWinds incident, which was described in Quarterly Report on Global Security Trends in the 3rd Quarter of 2020 [33], several companies that used Orion Platform, a popular piece of operation monitoring software, trusted its developer, SolarWinds, Inc, and downloaded and installed an update program falsified by an attacker. As a result, the attacker entered their systems and caused damage. As experienced in the incidents at SolarWinds, Inc and Mercari, Inc., a software supply chain attack can still occur, even if you use a software application supplied by a developer that is trusted by other user companies.

Supply chain attacks are divided into organizationally-linked supply chain attacks, which go through sales channels, and software supply chain attacks. Countermeasures against each type of attack are complex, as both involve several different organizations. The US's National Institute of Standards and Technology (NIST) published SP800-161, a document related to the risk management of supply chains, and is now revising the document in response to Presidential Decree No.13873. The European Union Agency for Cybersecurity (ENISA) published *Threat Landscape for Supply Chain Attacks*, which provides the analysis results of 24 supply chain attacks and their solutions. This report describes solutions to supply chain attacks by dividing such attacks into those designed for user companies and those designed for developers. The following are some of the countermeasures designed for user companies.

- Monitor risks and threats concerning supply chains, based on internal and external sources of information as well as the knowledge acquired through the monitoring and reviewing of suppler performance
- Manage suppliers through the whole lifecycles of products or services, including products or components that are no longer produced or supported
- Classify the assets and information that are shared by suppliers or can be accessed by suppliers, and define appropriate procedures for accessing and handling them
- Incorporate all of these obligations and requirements into contracts and agree on subcontracting rules and potentially linked requirements
- Ensure that suppliers and service providers guarantee that neither hidden features nor backdoors are contained intentionally
- Define processes that manage changes in contracts with suppliers, such as changes in tools and technologies

It is ideal to implement these countermeasures thoroughly. However, even the implementation of the above extracted countermeasures is not so easy. It will probably be very difficult to cover all of the countermeasures at once. Therefore, the initial mandatory countermeasure is to prevent the production environment from being penetrated, as demonstrated in Mercari's incident. The first step is to limit the channels connected to the production environment to prevent attackers from entering the production environment and use multi-factor authentication to prevent spoofing. The second step is to prevent falsified source codes from being released. Even if attackers are prevented from entering the production environment, source codes can still be falsified, if the attackers are already inside

GitHub. If a malicious process designed to steal information about online banking or credit cards is embedded into source code in the repository, not only old account information, but also the latest account information and security codes for credit cards may be stolen, which will result in larger damage. As the automation of development advances, falsified source codes will be released automatically. In many cases, they will not be noticed until the actual damage occurs. It is necessary to check for falsified source code and malicious code before code release.

2.2.5. Conclusion

In Mercari's incident, a software supply chain attack was made to target Codecov, a relatively new cloud service for developers, and the attacker attacked the development environments of users of the service, one after another, in order to enter them. It is believed that the attacker made attacks, assuming a configuration in which multiple development cloud services were connected to the development environment and the production environment. For development models using continuous integration (CI) or continuous deployment (CD), their building, testing and releasing processes are more automated. If an attacker embeds malicious code into them to exploit the production environment, it is difficult to prevent and notice their attempt in advance.

If your security check mechanism for source codes fails to detect malicious code, as described in "2.2.4 Countermeasures," the key point for preventing the spread of its damage is how quickly you can respond to the incident after noticing that you have or may have been attacked. In Mercari's incident, Codecov revealed an incident of unauthorized access by a third party on April 15. The following day (April 16), Mercari initialized (disabled and replaced) the authentication information stored in the CI environment as its primary response. If the investigation of the invasion of GitHub and the CI environment, which were linked to Codecov, had been started at that point, the invasion could have been detected earlier and the initial response could have been taken earlier than the start of the response made after being contacted by GitHub on April 23. When you notice that your system may have been attacked, the first step of your incident response should be to investigate the incident as far as the destinations linked/connected to the attacked system, find any signs of the attack and identify the range of its damage accurately. Mercari's initial response was relatively quick and it should be used as a good reference, as there are many cases in which such an opportunity cannot be used effectively and there is a delay in detecting and responding to the incident.

3. Data Breach

On May 21, 2021, Net Marketing Co. Ltd. revealed that fraudulent access was made from an external environment to the server that managed Omiai, a matchmaking application helping its users find a boyfriend/girlfriend and future husband/wife. Information submitted for age verification leaked, including image data of their driver's licenses, health insurance cards, passports and Individual Number Cards [34] [35]. This chapter describes the risk of exploitation of leaked ID image data, including driver's licenses, by malicious third parties in terms of eKYC, which was introduced in the Outlook section of the Quarterly Report for the 4th quarter of 2020, and each of the articles in the Act on Prevention of Transfer of Criminal Proceeds, which regulates eKYC.

3.1. Omiai Data Breach

Image data in age verification documents submitted by up to 1,711,756 people leaked from Omiai, which was operated by Net Marketing Co. Ltd. Omiai verified the ages of its applicants by using their driver's license and other ID image data in accordance with the Act on Regulation on Soliciting Children by Using Opposite Sex Introducing Service on Internet (Online Dating Site Act)." For that reason, the ID image data stored in Omiai has the following characteristics:

- Face photos of people aged 18 and over
- Highly reliable public ID cards
- High-resolution data captured by smartphones

It was an unprecedented incident of a personal data breach in which high-resolution image data on such highly reliable public ID cards leaked and affected over 1 million people. If a malicious attacker manages to obtain the highly reliable public ID data of over 1 million people, what criminal acts do they commit by exploiting such data?

For example, since people aged 18 and over fall into the category of working ages, the attacker can identify contact details of their target, based on the target's image data, and commit fraud to steal assets owned by the target. Also, when the attacker has the high-resolution image data of over 1 million people, which is obtained from highly reliable public ID cards, the attacker may be able to forge ID cards and pretend to be the target. According to the released information, driver's licenses accounted for about 60% of the leaked image data, which affected about 1 million people. Driver's licenses are often used as ID cards for identity verification. It is likely that you have also presented your driver's license before to verify your identification to someone, when receiving your mail or a delivery, issuing a membership card at a retailer, etc. The identity verification method using ID cards is also becoming a common method of identity verification for Omiai and other online services. The following section examines how the society may be affected , if high-resolution image data on ID cards can be exploited.

3.2. Unauthorized Use of Leaked Image Data on ID Cards

3.2.1. eKYC Standard

The existing identity verification method using ID cards is becoming more common as a method used when applying for an online service. As online services such as cloud services become more common among users, more users also want to complete their account verification online. However, when identity verification is completed online, can the identity of the applicant really be verified? Wouldn't the reliability of the verification be a concern? Companies providing online services will probably not issue accounts, unless proper identity verification is ensured. If suspicious users can disguise their identity and create fake accounts, online service providers will face serious problems such as the use of accounts for their online services in crimes and a failure to collect usage fees.

What is identity verification? The Ministry of Economy, Trade and Industry (METI) defines that it can be established in two ways: "identity proofing," which confirms the existence of a certain user, and "authentication," which confirms that the user is actually performing a certain operation [10]. For details, refer to "2.1.2. What is identity verification?" in the Quarterly Report for the 2nd quarter of 2020, which provides a detailed explanation. eKYC (electronic Know Your Customer) is an identity verification mechanism that uses ID cards to perform online or other non-face-to-face verification. As FinTech became more common, its identity verification procedure was regarded as a problem when opening accounts at online banks and online securities companies. On November 30, 2018, the Act on Prevention of Transfer of Criminal Proceeds was amended so as to allow for online identity verification using a non-face-to-face method. The main characteristic of eKYC is that it allows the user to use a PC browser or smartphone application to complete their identity verification quickly, completely online. eKYC improves the convenience of applicants by shortening the time required for their identity verification and simplifying its procedure. It also allows service providers to make the operation of identity verification more efficient and reduce the identity verification cost. However, while the online-completed procedure makes the operation faster and more convenient, it also seems to allow for some risk of spoofing using sophisticatedly forged ID cards [36].

When the Act on Prevention of Transfer of Criminal Proceeds (hereinafter "Criminal Proceeds Act") was amended, a standard for eKYC was provided in Article 6-1-1. Based on the description of eKYC, its characteristics are summarized in Table10. The Criminal Proceeds Act classifies eKYC into four categories.

Table10: eKYC Standard [37] [38] [39] [40]

Clause	Type	Identity verification method	Resistance to forged ID card	Service using each method
E	Selfie upload	Photo of ID card + Photo of face	△ Spoofing may be successful	・Bank ・Securities company ・Consumer finance company ・Communication carrier
F		Reading of IC chip + Photo of face	◎ Spoofing is difficult	Some banks
G	Federation	1. Photo of ID card + Query about customer information to bank, etc. / Credit card verification	○ Spoofing can be successful with some conditions (if bank account is available)	Credit card
		2. Reading of IC chip + Query about customer information to bank, etc. / Credit card verification	◎ Spoofing is difficult	
M		Public personal authentication / Use of Individual Number Card (reading of IC chip)	◎ Spoofing is difficult	・e-Tax ・Some securities companies ・Some payment settlement applications

Currently, Type-E is the most common and also used to open bank accounts online. However, identity verification using the Type-E method is the most vulnerable to spoofing using forged ID cards. Some banks use the Type-F method by reading IC chips, which is a securer method. For example, a driver's license with an IC card can be verified by comparing the information stored in the chip with the information entered online. Even if the face of the card is forged, it can be detected by using the correct information obtained from the IC chip. It is a securer method.

Credit card companies use Type-G methods. Depending on the identity proofing method used, Type-G methods are further divided into two patterns as shown in Table10: 1. Photo of ID card and 2. Reading of IC chip. Like Type-F, the method based on "2. Reading of IC chip + Query about customer information to bank, etc." is securer than the method based on "1. Photo of ID card + Query about customer information to bank, etc." For example, when this method is used to screen an applicant who is applying for a credit card, their identity is verified by comparing the information entered upon the application with the information that is already registered to the bank, including the applicant's address and birthday. If the applicant does not have any account with a trustworthy bank that coordinates the eKYC process with the

credit company, the identity of the applicant cannot be verified.

The Type-M method is an identity verification method using Individual Number Cards. It is used mainly by e-Tax, some securities companies and payment settlement applications. With a Individual Number Card, the identity of the holder is verified based on possession of the card and their knowledge of the password required to read the IC chip on the Individual Number Card. For example, when an applicant opens an account with a securities company, their Individual Number Card is set in an IC card reader and encrypted information about their application for opening an account is sent to the securities company, along with the information before the encryption, a public key and an electronic certificate for the applicant's signature. The securities company uses the received public key to decrypt the encrypted information and compares it with the information before the encryption to detect any falsification and make an inquiry about the validity of the electronic signature certificate to the signature certification authority to verify the identity of the applicant. As described above, it is difficult to forge a Individual Number Card with an IC chip. This eKYC method can also verify a valid Individual Number Card using an electronic signature certificate. Therefore, of all the eKYC methods listed in Table10, it is the most reliable identity verification method.

3.2.2. Performance of Type-E judgment method based on eKYC

Identity verification using eKYC also consists of the two processes of identity proofing and authentication. For example, "Photo of ID card" listed in the "E" row and the "Identity verification method" represents identity verification. Its result is combined with "Photo of face" to perform authentication.

If a forged ID card is misused and identity verification is attempted based on eKYC, how is authenticity judged? When you use the method that judges authenticity by photographing an ID card, you are probably operating on the assumption that attack methods will use a photocopied ID card. In addition to the clearness of the photo and text on the ID card, whether the ID card has any thickness is also used as another method for judging the authenticity of the ID card. In Japan, it is almost impossible to obtain reliable image data of other people's public ID cards such as driver's licenses. According to the National Police Agency of Japan, known cases of document forgery have been on the decline in recent years. This suggests that it is difficult to forge ID cards in Japan [41]. Even if a lost ID card is misused, its exploitation and forgery may still be detectable when the card is checked against an expiry list supplied by a credit record institution, etc. For this reason, it can be imagined that lost or stolen ID cards are not used for forgery in many cases. It is surmised that the reliability of judgment of ID cards has been ensured in the past, because it is difficult to forge reliable public ID cards and even the simple method for detecting forgery by photographing ID cards can reduce successful identity verification using a forged ID card to a certain level.

However, the incident of the Omiai data breach suggests that if massive high-resolution image data of reliable public ID cards leaks out, criminal syndicates may use such image data to forge ID cards with high precision, and more forged cards may circulate. If this

happens, the Type-E judgment method in Table10 can no longer detect forged ID cards. In the near future, online services using the Type-E judgment method based on eKYC may be tricked into approving account opening applications using forged ID cards. As a result, it is predicted that new spoofed accounts will increase. Especially, if the method is used by online banks and securities companies to open accounts, cases of its exploitation in crimes such as scams and money laundering may increase. Applicable financial institutions should consider monitoring fraudulent deposits and withdrawals and reviewing their identity verification methods. For other online services, changing to a more reliable method can also reduce the risk of receiving malicious spoofing attacks.

3.2.3. Performance of Type-F and Type-G2 judgment methods based on eKYC

The Type-F and Type-G2 judgment methods based on eKYC read the IC chips on ID cards. For example, since it is very difficult to forge IC card licenses, attempts for identity proofing using a forged IC card license fail. Therefore, these two judgment methods will not be affected by attacks as made in the incident of the Omiai data breach. Both methods guarantee the reliability of identity verification. The IC chip on an IC card license also records the data displayed on the front side of the license, such as the birthday and face photo, as well as the information that is not displayed on the front side, such as the legal domicile and nationality. The Type-F judgment method based on eKYC, which combines reading of the IC chip with the face photo on the card, compares the face photo data in the IC chip with the photographed face image of the applicant. Therefore, if the photo on the front side of the IC card license is replaced with a different one, that can be detected in the authentication process. The Type-F and Type-G2 judgment methods using IC card licenses can prevent fraudulent use of forged licenses with a fake front side and also prevent attackers from opening new spoofed accounts.

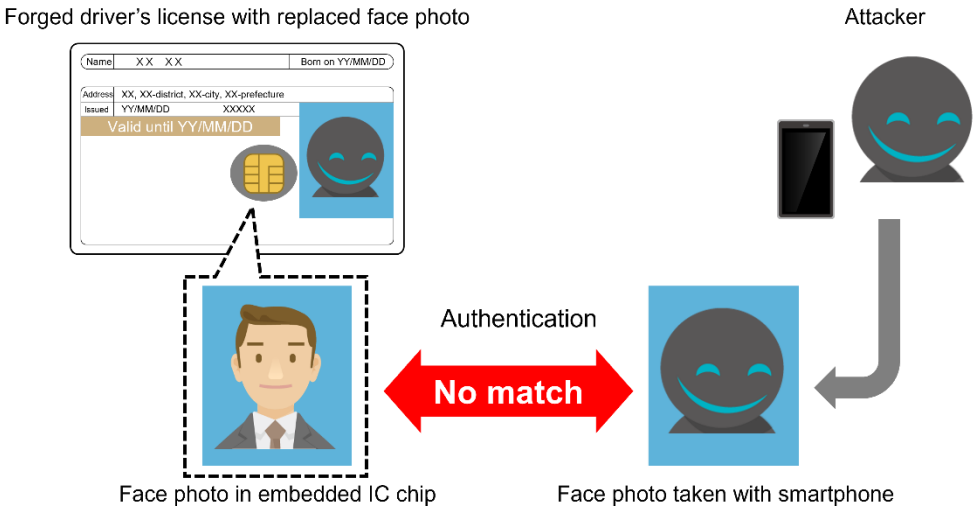


Figure 9: Type-F and Type-G2 Judgment Methods based on eKYC [42]

3.2.4. Performance of Type-G1 and Type-M judgment methods based on eKYC

If identity verification is performed by using an ID card that has been forged based on the leaked image data of another ID card, can that be detected by eKYC methods other than the three explained above? Results of our original evaluation are summarized in “Resistance to forged ID card” on in 3.2.1.

The Type-G1 method combines a photo of the ID card and a query to a bank, credit card company or other organization. As this method cannot detect a forged front side in a photo of an ID card easily, it is less resistant to forged ID cards than the methods that read the IC chip. There are two ways to make a query about customer information to a bank or credit card company. The first way is to use the identity information kept by a bank or credit card company. For example, you can connect to online banking in the middle of identity verification based on eKYC and compare the information entered in advance with the information registered to the online banking service, such as the name, address and birthday to perform identity proofing [43]. The second way is to use the data recorded in the passbook. A service provider such as a securities company transfers a certain amount of money to an existing bank account under the name of the applicant, and then the applicant checks the transferred amount of money and reports it to the service provider to complete authentication. In both ways, it is difficult to detect spoofing, if a forged ID card is used to prepare a bank account beforehand.

The public personal authentication method using a Individual Number Card in Type-M uses an electronic certificate for identity verification. Electronic certificates include “electronic certificates for signatures” and “electronic certificates for user certification.”

An electronic certificate for a signature can be used to check that the applicant has actually transmitted the target information on the Internet and also that the information has not been falsified.

This mechanism is described in Figure 10. For example, when applying to open an account, etc., the user sets their Individual Number Card in an IC card reader and enters their password. Then, the private key stored in the IC chip on the Individual Number Card is used to encrypt the application information in the IC chip (Figure 10-(1)). The encrypted application information (cryptogram) is sent to the service provider, along with the application information before the encryption, a public key and an electronic certificate for the applicant’s signature (Figure 10-(2)). The service provider can detect any falsification by decrypting the encrypted application information (cryptogram) with the received public key and comparing it with the application information before the encryption (Figure 10-(3) (4)). The service provider also makes an inquiry about the validity of the electronic signature certificate to the Japan Agency for Local Authority Information Systems (hereinafter “J-LIS”), which is a signature certification authority. J-LIS checks it against expiry information and returns its result (Figure 10-(5)). If the electronic signature certificate is valid, the identity verification is successful (Figure 10-(5)).

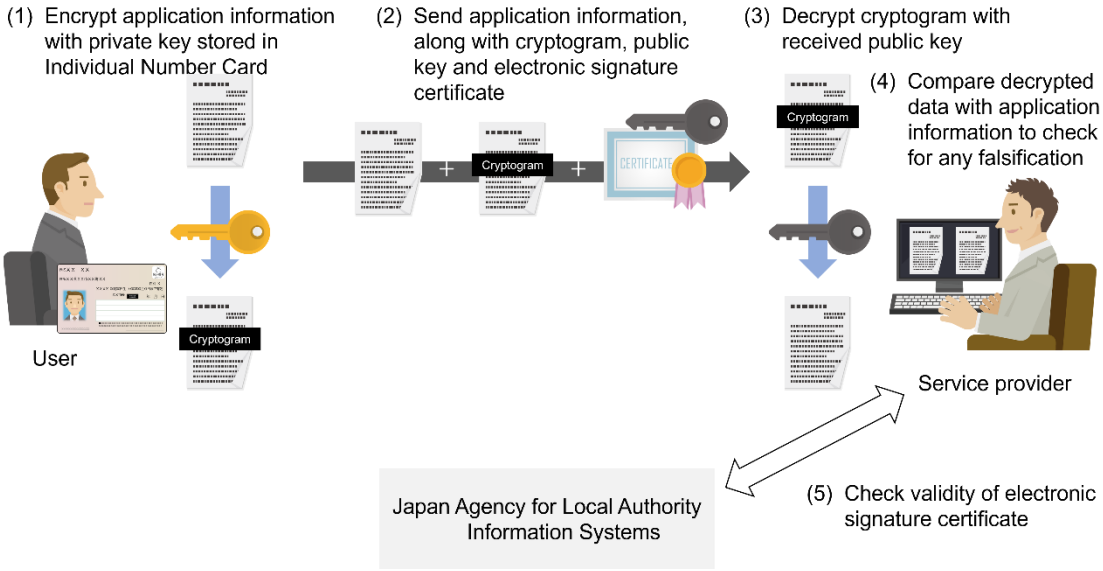


Figure 10: Mechanism of Public Authentication Service Using Electronic Signature Certificate [44]

Electronic certificate for user certification can be used to certify the user's identity. For example, if the user needs to verify their identity when opening an account, the user enters their password and uses the private key in the IC chip on their Individual Number Card to encrypt the random number sent by the service provider in the IC chip, in the same manner as for the electronic signature certificate (Figure 11-(2)). The user returns the encrypted random number, the random number before the encryption, an electronic certificate for user certification and a public key (Figure 11-(3)). The service provider can detect any falsification by decrypting the encrypted random number (cryptogram) with the public key and comparing it with the random number before the encryption (Figure 11-(4) (5)). In the same manner as for the electronic signature certificate, the validity of the electronic certificate for user certification is checked and its result is received (Figure 11-(6)). If the electronic certificate for user certification is valid, the identity verification is successful (6)).

The eKYC method using a Individual Number Card in Type-M uses either an electronic certificate for a signature or an electronic certificate for user certification to perform identity proofing.

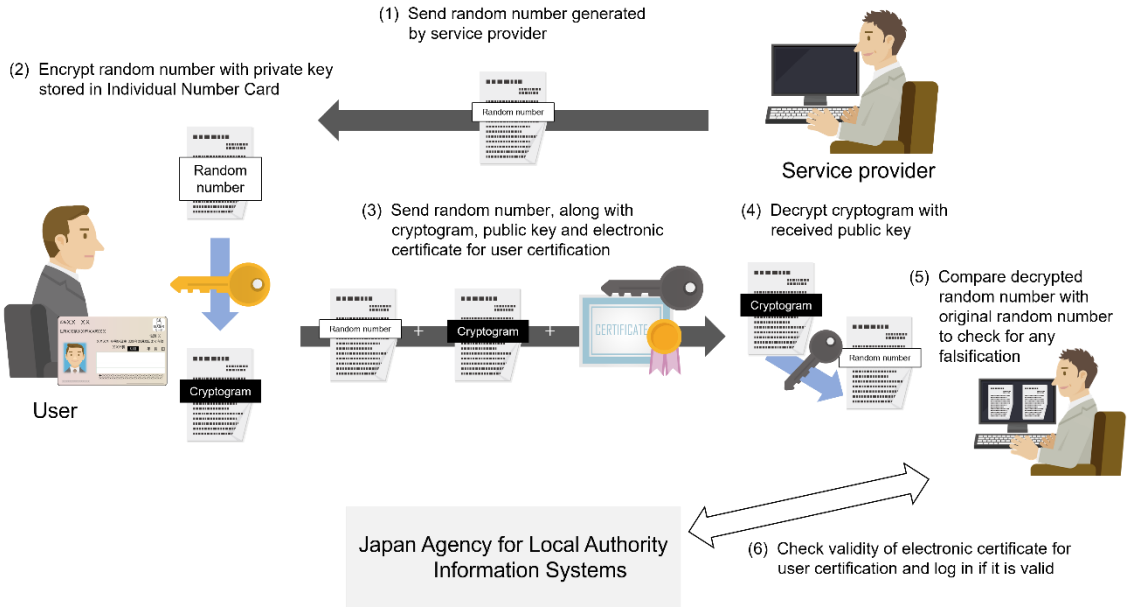


Figure 11: Mechanism of Public Authentication Service Using Electronic Certificate for User Certification [44]

3.2.5. Impact on Conventional Identity Verification

There is some concern that the leakage of image data on driver's licenses in the incident of the Omiai data breach may affect not only identity verification using eKYC, but also conventional identity verification.

When image data of a driver's license leaks out, personal information such as the holder's name, address, birthday and face photo can be obtained from the image data. As long as such information is available, some financial services allow you to complete the identity verification required to open an account. Leakage of such information may cause larger damage than leakage of IDs and passwords in the future. Because of this incident, the risk of attacks may also increase in conventional identity verification that uses only a copy of a driver's license to examine the application. The incident may also affect certified mail with delivery restricted to the addressee, which uses an ID card to verify the identity of the addressee. A skilled crime syndicate may be able to forge a driver's license by replacing the face photo and address on it with fake data, present the driver's license with the forged front at the post office, pretending to be the addressee, and receive the mail successfully. When attackers try to pretend to be someone else, they exploit the most vulnerable identity verification method. Companies also need to review their conventional identity verification methods.

3.3. Conclusion

"Secondary damage of data breach incidents to beware of" in the Outlook section of the Quarterly Report in the 4th quarter of 2020 stated that companies must calculate the risk of

spoofing in their own services and implement countermeasures to prevent, reduce or accept such a risk.

As indicated in crime statistics released by the National Police Agency, it is difficult to forge ID cards, and until recently, there has been very little concern about spoofing using an ID card with a forged front during identity verification by photographing the ID card. However, crime syndicates may be able to use the image data of ID cards leaked in the incident of the Omiai data breach to forge ID cards with high precision. Companies should monitor their own services for spoofing and review their identity verification methods, if spoofing occurs frequently.

It is believed that in the future, Type-F, Type-G2 and Type-M based on eKYC, which read IC chips to detect forged ID cards, will become more commonly used, instead of the methods that photograph ID cards.

4. Vulnerabilities

Vulnerabilities are hiding in something we are all familiar with and which readers of this document probably use regularly. Do you know what it is? In May 2021, Mr. Mathy Vanhoef at New York University Abu Dhabi (hereinafter “Mr. Vanhoef”) revealed that IEEE 802.11, which is one of the most commonly used international standards for wireless LAN, had multiple vulnerabilities [45] [46]. These vulnerabilities exist in all wireless LAN devices that belong to IEEE 802.11, and any user of a wireless LAN device may be attacked. This chapter explains what vulnerabilities Mr. Vanhoef discovered and how they should be dealt with.

4.1. Overview of FragAttacks

The multiple vulnerabilities discovered by Mr. Vanhoef are collectively called “FragAttacks (**fr**agmentation and **ag**gregation **attacks**)” [47]. Some of these vulnerabilities have been undetected and existed for more than 20 years, since the Institute of Electrical and Electronics Engineers (IEEE) released its first wireless LAN standard in 1997 [45].

The technical specifications of most wireless LAN devices are determined in compliance with IEEE 802.11, and their interoperability with competitor devices is tested by an industrial association called “Wi-Fi Alliance” [5]. To put it plainly, any wireless LAN device that has obtained Wi-Fi certification from the Wi-Fi Alliance [48] is subject to FragAttacks. In other words, all wireless LAN devices that communicate through Wi-FI and all Wi-Fi users are subject to such attacks [45] [48]. WEP, WPA3 and other protocols that improve the security of wireless LAN are also subject to FragAttacks, as they comply with IEEE 802.11. For a long time, vulnerabilities have been hiding in Wi-Fi, which is something we are very familiar with.

To make FragAttacks, however, the attacker needs to be within the same area as the target wireless communication and the attack method is also very complicated. Since FragAttacks were revealed, therefore, there have been no reported cases of attacks on such vulnerabilities. Nonetheless, we cannot deny the possibility of related damage in the future, if attackers use FragAttacks information to develop tools that attack these vulnerabilities.

4.2. Cause of FragAttacks and Attack Mechanism

As described in 4.1, FragAttacks are named by combining Frame aggregation and Frame fragmentation. FragAttacks are vulnerabilities derived from design and implementation defects in the standard for wireless LAN devices [49]. There are one design vulnerability related to Frame aggregation, two design vulnerabilities related to Frame fragmentation [45], and several implementation vulnerabilities linked to the design vulnerabilities.

How can attackers attack these vulnerabilities?

4.2.1. Aggregation Attack

This section describes Aggregation attacks that exploit a design insufficiency in Frame aggregation (CVE- 2020-24588) [45] [50]. Frame aggregation is a transmission method that arranges one or more frames in the 802.2/802.3 format into a single frame in the IEEE 802.11 format and sends it efficiently through Wi-Fi [1]. The frame header for the IEEE802.11 format has the A-MSDU (Aggregate MAC Service Data Unit) flag, which indicates an integrated frame consisting of one or more A-MSDU frames. For an integrated frame, the A-MSDU flag is set to 1. In IEEE 802.11, the A-MSDU flag ("is aggregated" in Figure 12) is not protected and a third party can rewrite the A-MSDU flag maliciously . This allows the attacker to set the A-MSDU flag to a single frame in the IEEE 802.11 format, make the single frame look like an integrated frame consisting of one of more A-MSDU frames, and send it to the recipient. Then, the attacker changes the value of the frame length, which is contained in the header of the A-MSDU frames that look like an integrated frame. The attacker can add frames to match the changed frame length. The attacker can embed an attack in the added frames.

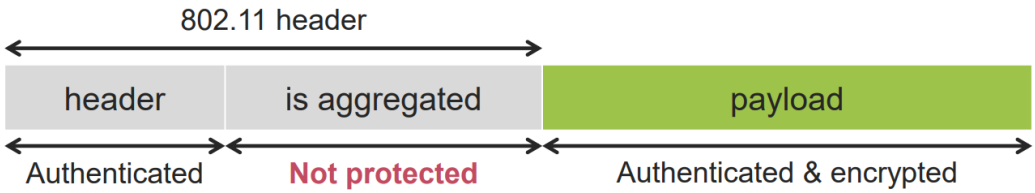


Figure 12: Frame of Data Sent in IEEE 802.11 [47]

For example, the attacker can use this method to enter an attack packet exploiting ICMPv6 RA (Router Advertisement) into a frame and delivers it to the device that they want to attack. If the device to be attacked is an IPv4/IPv6 dual stack, the OS setting is changed so that the malicious DNS server prepared by the attacker is used when the attack packet exploiting ICMPv6 RA is received. When the user tries to access a website on the Internet, the device to be attacked requests name resolution to the malicious DNS server, which was prepared by the attacker. Then, the attacker's DNS server provides a fake IP address and the user is directed to a phishing site prepared by the attacker. For example, when the user wants to shop at Amazon and enter "www.amazon.com" in their browser, the device requests name resolution to the malicious DNS server. Then, the attacker's DNS server returns the IP address of the phishing site prepared by the attacker to the device, instead of the genuine Amazon IP address. As the user is directed to the malicious phishing site that was prepared by the attacker and looks identical to the genuine site, the user enters their ID and password. As indicated above, the attacker can make a phishing attack easily on the user of the IPv4/IPv6 dual stack device connected to Wi-Fi.

4.2.2. Mixed key Attack

This section describes attacks that exploit two vulnerabilities derived from design insufficiencies in frame fragmentation [1]. Frame fragmentation is a transmission method that uses IEEE 802.11 to divide a large-sized packet into multiple fragmented packets during the transmission of data and place them in a frame to send the data [45].

Let's take a look at the Mixed key attack that exploits the first vulnerability (CVE2020-24587) to frame fragmentation. With frame fragmentation, the transmission side divides one packet into multiple fragmented packets, and then encrypts each of the divided, fragmented packets with the cryptographic key "k," places them in a frame and sends the data to a wireless LAN access point (hereinafter "AP"). In IEEE 802.11, even if a frame containing fragmented packets encrypted with the cryptographic key "k" coexists with a frame containing fragmented packets encrypted with the cryptographic key "m," AP can receive both frames and decrypt each fragmented packet with its corresponding cryptographic key, which causes a problem [50]. AP connects the decrypted packets to reconstruct each packet and sends that packet to the destination specified in the header of the packet. If the attacker can relay Wi-Fi, the attacker uses the above method to place the frame sent by the device to be tapped together with a different frame and reconstruct a packet that contains information about the device to be tapped. Then, they receive that packet and steal the information.

The following is a description of the Mixed key attack. First, the attacker makes the device to be tapped access an Internet website prepared by the attacker. At this time, the attacker cuts in between the device to be tapped and the wireless LAN access point (hereinafter "AP") to relay the communication. In other words, the attacker prepares a condition that allows for a Man-In-The-Middle (MITM) attack. When the device to be tapped accesses the attacker's website, a long domain name, FQDN or URL is specified as the destination so that packet division occurs (fragmentation). Then, the device to be tapped divides the packet into multiple fragmented packets, encrypts them with the cryptographic key "k", then places them in multiple frames and sends them.

Next, the attacker receives the above multiple frames. The attacker obtains the fragment number and sequence number "s" of the first frame ("Enck{Frag0(s)}" in Figure 13) and transfers them to AP as they are. The second and succeeding frames are not transferred to AP, but discarded instead. AP saves the first frame in its memory and waits for the arrival of the second and succeeding frames.

The device to be tapped and AP change the cryptographic key at certain intervals. When the cryptographic key changes to "m", the attacker receives multiple frames containing the fragmented packets sent by the device to be tapped. Then, the first frame ("Encm{Frag0(s')}" in Figure 13) is discarded. The second and succeeding frames ("Encm{Frag1(s')}", "Encm{Frag2(s')}"…in) change their header sequence number "s'" to "s" to match the first relayed frame "Enck{Frag0(s)}" . Then, the second and succeeding malicious frames are transferred to AP.

Finally, AP decrypts the first frame saved in the memory "$Enc_k\{Frag_0(s)\}$" and the second and succeeding frames in the other communication "$Enc_m\{Frag_1(s)\}$, $Enc_m\{Frag_2(s)\}$...$Enc_m\{Frag_x(s)\}$" with the cryptographic keys k and m, respectively, to reconstruct the divided packet. In other words, the attacker places the packet header part

of the destination of the attacker's website in the first frame, places the fragmented packets sent by the device to be tapped into the second and succeeding frames, and then sends them in order. Then, AP decrypts the encryption and combines the headers and payloads of the different packets to generate a packet. As the generated packet is sent to the attacker's website, the attacker can obtain information about the device to be tapped from the payload part. Repeating this allows the attacker to steal useful information from the device to be tapped [45] [47]. The multiple divided frames (fragments) are temporarily stored in AP's memory so that they can be processed. This vulnerability occurs because neither the deletion timing nor control method for such frames is determined.

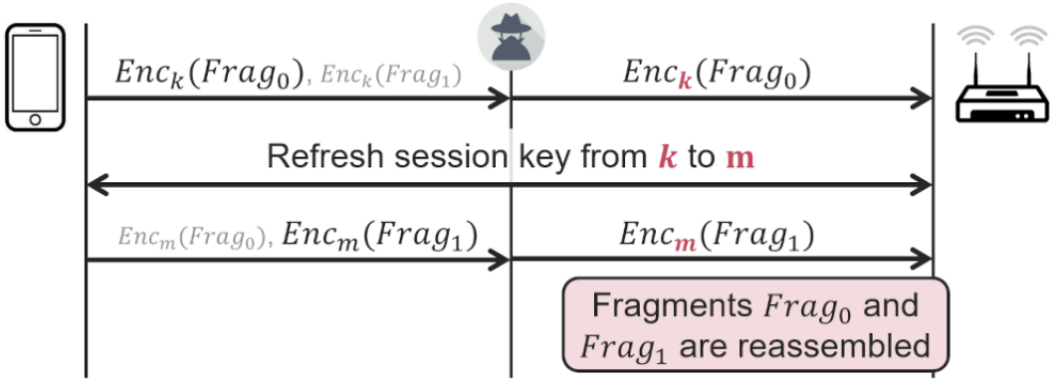


Figure 13: Flowchart of Mixed Key Attack [47]

4.2.3. Fragment Cache Attack

Attack that exploits the second vulnerability of frame fragmentation (CVE2020-24586) is called "fragment cache attack." In IEEE 802.11, if the communication is blocked during the reconstruction of multiple frames containing fragmented packets for some reason, the frames that are in the middle of the reconstruction remain in AP's memory. The attacker sends a malicious frame to AP, reconstructs the contained fragmented packets along with the remaining frames, and then takes them out. This attack poisons the fragment cache.

The following is a description of the fragment cache attack.

First, the attacker spoofs the MAC address of the device to be tapped and connects to AP, then prepares a condition that allows for a Man-In-The-Middle attack. The device to be tapped sends the authentication frame for AP connection whose destination is specified as the attacker. The attacker extracts only the beginning of the authentication frame, creates an encrypted frame ("Enck {Frag0(s)}" in Figure14), and sends it to AP. Then, AP decrypts this frame and saves the extracted fragmented packet "Frag0(s)" to the memory. The attacker sends a disconnection notification to AP and disconnects Wi-Fi.

Next, the attacker connects to AP again and prepares a condition that allows for a Man-In-The-Middle attack just like the first time. Since IEEE 802.11 has no specification that stipulates the deletion of any fragmented packet that is saved when the client is disconnected or reconnected, the fragmented packet "$Frag_0$(s)" remains in AP's memory. The fragmented packet "$Frag_0$(s)" becomes the first fragmented packet. When the device to be tapped sends

multiple divided frames, the attacker receives them and discards the first frame (”Encl (Frag0(s’))” in Figure14). The second and succeeding frames (”Encm (Frag1(s’))”, ”Encm (Frag2(s’))”… in) change their header sequence number ”s’” to ”s” to match ”Frag0(s)”, which remains in AP’s memory. Then, the second and succeeding malicious frames are transferred to AP.

Finally, like the step in 4.2.2 Mixed key Attack, AP decrypts ”$Frag_0$(s)”, the first fragmented packet stored in the memory, and ”Enc_m{$Frag_1$(s)}, Enc_m{$Frag_2$(s)}...Enc_m{$Frag_x$(s)}”, the second and succeeding frames received afterwards, with the cryptographic key m and connects the extracted, fragmented packets to reconstruct a packet. As the destination of the first packet is specified as the attacker, AP sends the reconstructed packet to the attacker. When the attacker receives this packet, the attacker can obtain information about the device to be tapped from its payload part. Like the step in 4.2.2 Mixed key Attack, the attacker repeats this and steals useful information from the device to be tapped.

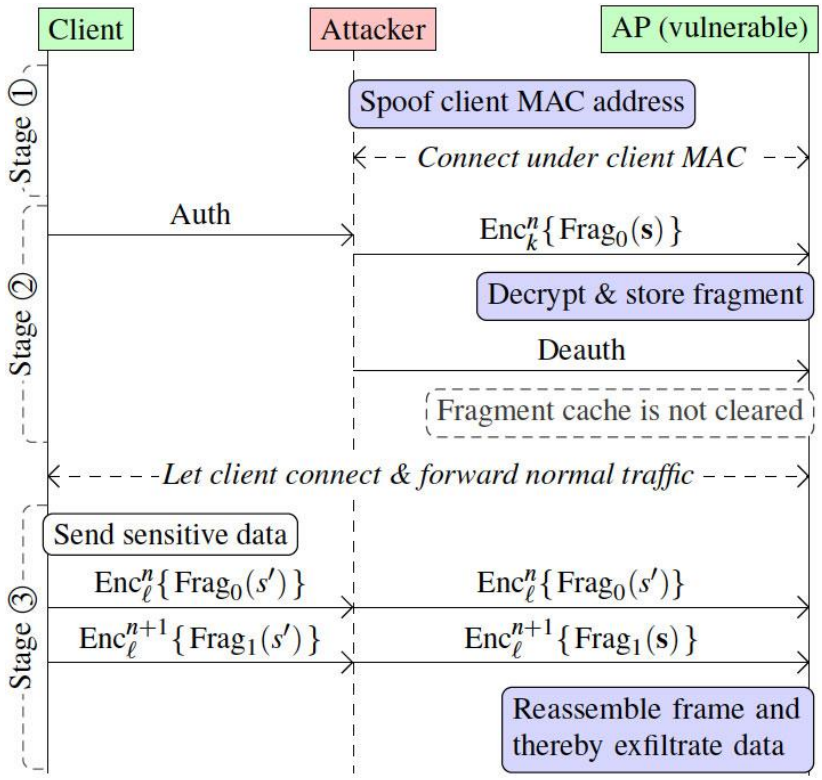


Figure14: Flowchart of Fragment Cache Attack [45]

According to information released by the Wi-Fi Alliance, IEEE802.11 has a total of 12 design and implementation vulnerabilities [51]. In addition to the three design vulnerabilities, which are described above, IEEE802.11 has nine implementation vulnerabilities. The following table lists the 12 vulnerabilities according to the base value of CVSS v3, provided by the National Vulnerability Database(NVD), in the order from the highest to the lowest value . The base value is obtained by calculating the severity of each vulnerability according to the basic characteristics of the vulnerability.

Table11: List of Vulnerability FragAttacks [53]

CVE number	CVSS v3 Base value	Description of vulnerability	Problem type
CVE-2020-26139	7.8	Even if the sender is not authenticated, EAPOL is exploited to transfer frames.	Implementation insufficiency
CVE-2020-26142	7.5	Fragmented frames are processed as full frames.	Implementation insufficiency
CVE-2020-26140	6.5	Plaintext data frames are accepted in protected networks.	Implementation insufficiency
CVE-2020-26141	6.5	TKIP MIC of fragmented frames is not verified.	Implementation insufficiency
CVE-2020-26143	6.5	Fragmented plaintext data frames are accepted in protected networks.	Implementation insufficiency
CVE-2020-26144	6.5	Plaintext A-MSDU frames that have the RFC1042 header in which EAPOL is specified as EtherType are accepted in encrypted networks.	Implementation insufficiency
CVE-2020-26145	6.5	Plaintext broadcast fragments are accepted as full frames in encrypted networks.	Implementation insufficiency
CVE-2020-26147	5.4	Encrypted fragments and plaintext fragments are mixed and reassembled.	Implementation insufficiency
CVE-2020-26146	5.3	Encrypted fragments that have discontinuous packet numbers are reassembled.	Implementation insufficiency
CVE-2020-24586	3.5	As the fragment cache is not cleared from the memory during network reconnection, the attacker steals packet content under certain conditions.	Design insufficiency
CVE-2020-24587	3.5	As fragments encrypted with different keys are reassembled, the attacker can steal packet content under certain conditions.	Design insufficiency
CVE-2020-24588	2.6	As the frame aggregation flag in the header is not protected, the attacker can rewrite the header information and insert a malicious packet.	Design insufficiency

4.3. Conclusion

Until now, there have been no reported attacks on FragAttacks vulnerabilities. This is because it is difficult to meet the preconditions required to execute FragAttacks and it is also costly to do so. The attacker needs to get close to a distance in which they can receive the radio waves used by the device to be attacked and its Wi-Fi AP, and also needs to install the equipment for their attack. If there is any restriction on physical entry into the premises or building, the attacker cannot get close to a distance in which they can receive the radio waves from the attack target. Also, when the distance from the attack target is 300m, the Wi-Fi frame arrival time is delayed by 1μs. Since a Man-In-The-Middle attack requires the time for producing a malicious frame, which further delays the time from the reception to transmission of frames, the Man-In-The-Middle attack tends to fail easily. A successful attack probably needs high-performance attacking equipment. To attack a number of targets, the cost for moving to attackable locations is also high.

Considering the above, it is unlikely to see FragAttacks cause massive damages all over the world. As, however, many vulnerable wireless LAN devices exist in the world, they should not be left unprotected. It is necessary to raise the awareness of this issue among as many wireless LAN administrators and Wi-Fi users as possible. Industrial associations for Internet security such as ICASI and the Wi-Fi Alliance introduce the advisories issued by vendor companies, publish articles that describe the necessity of countermeasures and release various information on FragAttacks [51] [54]. However, it will be impossible for them to direct all users to apply patches to all wireless LAN devices in the world. It is likely that many users in the world don’t know how to apply patches. Furthermore, many wireless LAN devices have likely been running without their administrators. It is believed that this problem cannot be solved completely in the near future, unless there is a mechanism that applies patches to all wireless LAN devices automatically. It will take a very long time to solve it.

5. Malware/Ransomware

5.1. Summary of 1st Quarter of 2021

Reports on damage cases caused by malware and ransomware continue from 2020. There has been an increase in attacks on infrastructure companies, which significantly affect people's lives when attacked. On May 7, Colonial Pipeline (hereinafter "Colonial"), the largest petroleum pipeline company in the US, received a ransomware attack and stopped all of its pipeline operations [55]. On May 31, JBS, the largest meat company in Brazil, revealed that it had also received a ransomware attack [56]. This forced JBS to stop the systems of its meat-processing plants in North America and Australia.

This chapter examines the Colonial incident and describes the developments of the incident and Colonial's responses to it. The chapter also mentions the actions that the US and Japanese governments are taking against ransomware attacks.

5.2. Ransomware attack on Colonial

5.2.1. Overview

On May 7, 2021, Colonial, a US petroleum pipeline company, received a ransomware attack and stopped all of its pipeline operations [55]. Colonial is the largest infrastructure company in the US, and holds nearly half the market share of fuel consumption on the East Coast. This case was caused by "Darkside," an attacker group that makes double-extortion ransomware attacks [57]. Darkside demanded that Colonial pay the cryptocurrency equivalent of 4.4 million dollars as a ransom for the decryption of the encrypted data. Darkside also threatened to disclose the stolen data unless the company paid the ransom.

It was originally reported that Colonial had no intention to pay the ransom. Later, however, Colonial CEO Joseph Blount revealed that the company had paid the ransom, just as Darkside had demanded [58]. CEO Blount said that although he had known that paying the ransom would be a controversial act, he had made the tough decision, taking into the account the risk that the shutdown of the pipelines would significantly affect people's lives and economic activities [58] [59]. Actually, after the shutdown of the pipelines, the price of petroleum surged in the US and people panicked buying it, causing chaos. After paying the ransom, Colonial used the decryption tool provided by Darkside and its own backup system to recover the data, and resumed normal operation of the pipelines on May 15.

In the Colonial incident, the system was restored when the victim paid the ransom to the attacker group. However, the incident responses in this case did not end there. On June 7, the Federal Bureau of Investigation (FBI) recovered 63.7 bitcoins, equivalent to about 2.3 million dollars, from Darkside, out of a total ransom amount of4.4 million dollars. It was a rare case in which a portion of paid ransom money was successfully recovered as a result of an incident response to a ransomware attack. The timeline of the Colonial incident is as shown below.

Table 12: Timeline of Ransomware Attack on Colonial

Date	Status
5/6	The attacker group “Darkside” stole nearly 100GB of data from Colonial’s network within 2 hours [55] [61].
5/7	Colonial noticed that it had received a ransomware attack and stopped operating all of its pipelines. The company contacted the US government and FBI. It paid Darkside a ransom of about 4.4 million dollars.
5/10	FBI revealed that Darkside ransomware had been used for the attack.
5/15	Colonial resumed its normal pipeline operation.
6/7	The US Department of Justice announced that the FBI had recovered bitcoins equivalent to about 2.30 million dollars out of the ransom paid by Colonial.

5.2.2. Recovery of Ransom by FBI

How did FBI succeed in seizing some of the bitcoins paid for the ransom? Criminals immediately launder the cryptocurrency gained as a ransom from the cryptocurrency account into which the ransom is paid. Money laundering is an act of evading the discovery of a crime or an arrest by an investigation agency such as the police by moving the money that is illegally gained in a crime or illicit transaction, from one bank account to another that is either fictitious or under the name of someone else repeatedly, so as to hide its original source [62]. Ransomware attacker groups launder money by dividing ransom money into small portions and transferring them to multiple cryptocurrency accounts or converting the original cryptocurrency into another cryptocurrency.

The following three actions are required to recover laundered ransom money. In the Colonial incident, some of the ransom money was recovered successfully because the FBI was able to implement (1) to (3) below.

(1) Tracking the cryptocurrency and identifying the target account

The FBI used Blockchain Explorer, which allows the user to search Blockchain to ascertain the monetary amount of a certain transaction and its destination, to monitor Darkside’s money laundering [63] [64]. As a result, the FBI discovered that 63.7 bitcoins were deposited in one bitcoin account.

(2) Obtaining the private key for the bitcoin account

The FBI succeeded in obtaining the private key required to unlock the bitcoin account in which the ransom money was deposited. However, the FBI did not reveal how it was obtained. There are several speculations. Some people think that the FBI sent a spy to Darkside and obtained the private key, while others suspect that Darkside had a betrayer who leaked the key to FBI. However, it is most likely that the security of the storage server in which the attacker group managed the private key was slapdash [65].

(3) Seizing the cryptocurrency in the account

The FBI requested that the Federal District Court for the Northern District of California issue a warrant for the seizure of the ransom. In response, the court issued the warrant immediately. Then, the Special Prosecutions Section and Asset Forfeiture Unit of the US Attorney's Office for the Northern District of California seized the bitcoins deposited in a certain bitcoin account [66] [67].

It is believed that the above course of action was possible only because both the victim (Colonial) and the law enforcers such as the US government and FBI all collaborated together quickly. Tracking cryptocurrency is not an unusual investigation method. As, however, Colonial cooperated with the US government and law enforcers immediately after being attacked, the FBI managed to track the flow of the cryptocurrency thoroughly, starting from the point when the ransom was paid. It is believed that because the FBI regularly collects information about attacker groups and tracks the flows of cryptocurrencies, the FBI was able to make full use of the investigation techniques that it had developed over years, in the Colonial incident. As the FBI also managed to collaborate with the Californian court to issue a seizure warrant quickly, the US Attorney's Office was able to seize the funds smoothly. One of the reasons why Colonial was able to cooperate with the law enforcers to respond to the ransomware attack, as described above, was that the US government was increasing efforts against ransomware attacks such as advisories issued by the OFAC and the establishment of a ransomware attack countermeasure body.

5.2.3. Responses to Ransomware Attacks in the US

In the US, there is an increasing sense of impeding crisis regarding ransomware attacks, and the whole country is strengthening its responses to such attacks. As their concrete actions, this section describes the issuing of an advisory concerning the payment of ransoms and the establishment of a ransomware attack countermeasure body.

In October 2020, the Office of Foreign Assets Control (OFAC) announced an advisory concerning the payment of ransoms. This topic was introduced in the Quarterly Report for the 3rd quarter of 2020 [57]. The advisory states that an organization that paid a ransom to an attacker group must report the received attack to law enforcement immediately and cooperate with them, as the organization may be subject to a fine or punishment.

In January 2021, the Ransomware Task Force (RTF) was established as a ransomware attack countermeasure body in the US [68]. Ransomware attacks are increasing daily, and their scale is also expanding. Currently, however, there are not many organizations that take sufficient countermeasures. As a result, damage caused by ransomware attacks is increasing and also becoming more serious. To tackle this issue, the RTF was formed for the purpose of standardizing a framework of responding to ransomware attacks and fighting against such attacks in a cross-departmental manner. The RTF consists of more than 60 members, including large IT companies such as Amazon, Cisco and Microsoft, governmental bodies, law firms and academic organizations. The RTF has released the RTF Report, which summarizes the actions that governments and companies should take against ransomware

attacks [69]. The RTF Report sets the following four goals (quoted from [69]).

Table 13: Goals Set in RTF Report

Goal	Description
1. deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy	In order to deter ransomware attacks, each country must use its national power to commit itself to these actions and also cooperate with other countries internationally. Each country will be called on to increase the priority of its investigations on attacks and pressure the countries that hide attacker groups. Each country should also cooperate internationally to strive to take down ransomware.
2. disrupt activities by attacker groups	To reduce damage caused by ransomware attacks, it is also necessary to destroy business models established by attacker groups. This will reduce profits made by attacks and increase attackers' risks. Criminal prosecution and other methods will also be used to hunt down members of attacker groups.
3. help organizations prepare for ransomware attacks	Many organizations don't take sufficient countermeasures against ransomware attacks. Each organization will be supported so as to raise its awareness and implement countermeasures according to its own situation in order to obtain appropriate information.
4. respond to incidents of ransomware attacks more effectively	In quite a few cases, the victim pays a ransom in a hurry, fearing that the stolen data may not be recovered permanently or the organization may lose its public trust. It is important to create an environment where victims are aware that they should report the incident to their government and victims are also provided with appropriate support.

The RTF Report provides 48 recommendations to achieve the goals listed in Table 13 and many of them describe concrete methods for responding to attacks in a cross-departmental manner across the boundary between the government and private sector. As one of the recommendations to achieve goal 2, for example, the Report states that "Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading desks to comply with existing laws." Like in the case of Colonial, the attacker demands that the victim pay a ransom for the ransomware attack in a cryptocurrency. After the attacker group launders the cryptocurrency received as the ransom money, the cryptocurrency is converted into cash via a cryptocurrency exchange, etc. Therefore, the RTF Report requires that cryptocurrency exchanges and similar entities comply with laws concerning KYC (Know Your Customer), AML (Anti-Money Laundering) and CFT (Combatting Financing of Terrorism). If cryptocurrency exchanges implement these recommendations more, attacker groups cannot cash ransoms, because they cannot open accounts or launder the money at cryptocurrency exchanges.

5.3. Responses to Ransomware Attacks in Japan

5.2. described efforts against ransomware attacks in the US. 5.3 introduces the methods that the Japanese government and law enforcement are currently using to respond to ransomware attacks.

When a Japanese organization receives a ransomware attack and reports the incident, the cybercrime investigation unit or another section of each prefectural police department that handles cybercrimes plays the main role in investigating the incident. As, however, some local governments have very few staff members who are familiar with cybercrimes, the level of investigation varies depending on each prefectural police department and it is currently difficult to collaborate with companies, law enforcement or overseas investigation bodies. The cybercrime department of each prefectural police department has a limited ability to respond to the latest cybercrimes.

As the first step in solving this problem, the National Police Agency announced that a “Cyber Bureau” would be established in 2022 [70] [71]. The Cyber Bureau will centrally manage cyber-related cases, which are currently handled across the Community Safety Bureau, Security Bureau and other departments of the National Police Agency. In addition, a new specialist investigation force under direct management by the national government (Cyber Direct Control Force [provisional name]) will also be established, and about 200 investigators with special knowledge will be gathered from all over Japan to investigate serious cyberattacks. As the National Police Agency directly investigates cyber-related cases as a direct control force of the national government, the collection and analysis of information about cyber-related cases will improve, and investigation skills are expected to improve. This is also expected to facilitate both collaboration with the private sector and collaboration with other countries.

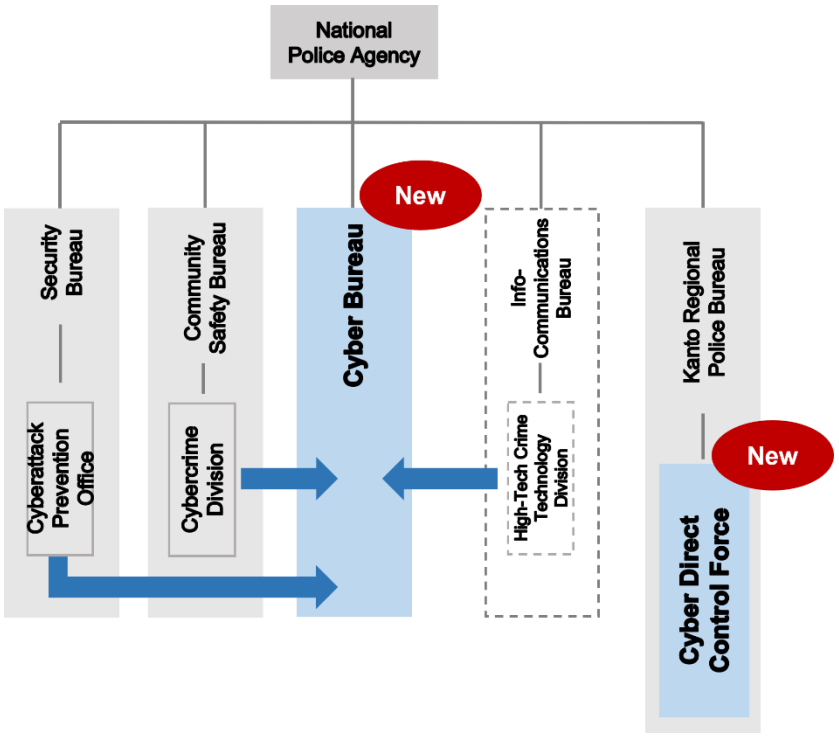


Figure 15: Conceptual Image of Proposed Reorganization of National Police Agency [72]

(Source data modified by the author)

However, it is not only the police investigation structure that must be strengthened. Japan needs to increase its nationwide responses to ransomware attacks. The first step will be to provide enough information to enable helping attacked organizations make appropriate decisions on the payment of ransoms and system recovery in the case they receive ransomware attacks and resultant damages. Unlike the US, it may be difficult to establish a structure that can recover ransom money. However, Japan should promote more countermeasures against ransomware to organizations that may receive the next ransomware attacks. To achieve this, Japan should establish a structure where both the government and the private sector can collaborate to deploy initiatives for promoting ransomware countermeasures from many different angles. In the same manner as the US promoted and deployed OFAC advisories and RTF recommendations, the Japanese government also needs to establish a cross-departmental organization consisting of each industry, law enforcement, judicial organs and administrative bodies, and give concrete directions in national initiatives for ransomware countermeasures.

5.4. Conclusion

This chapter examined the Colonial incident and described that it was an unusual case in which a portion of the paid ransom money was recovered successfully. Then, the chapter introduced the nationwide, cross-departmental commitment against ransomware attacks in

the US and made a comparison in efforts against ransomware attacks between the US and Japan.

The recovery of the ransom money in the Colonial incident was entirely a very special solution that took place after the payment of the ransom. The first ransomware countermeasure that you should take is to prevent ransomware attacks. Then, you should minimize the received damage, even if you are attacked. Organizations that don't have sufficient countermeasures should implement these two countermeasures first. Many organizations don't have sophisticated ransomware countermeasures. Particularly in Japan, the government needs to take the main role in increasing its responses to ransomware attacks. The government should be committed to the development of a structure that allows attacked organizations to collaborate with public institutions quickly and make cross-departmental responses. The first step the government should take is probably to develop an organization or mechanism on which attacked organizations can depend, before anything else. Japan needs a public-private support organization that provides enough information to attacked organizations to enable them to make appropriate decisions on system recovery and the payment of ransoms and also directs concrete actions that the attacked organizations should take in order to minimize the received damage.

6. Outlook

Criticizing countries associated with attacker groups by name

There is a growing trend among countries affected by cyberattacks to name and criticize the countries involved in the attacker groups and their crimes. In April 2021, the National Police Agency suspected that the People's Liberation Army of China had directed cyberattacks on Japanese research institutions and companies, including the Japan Aerospace Exploration Agency (JAXA), which occurred from 2016 to 2017 [73]. Not only Japan, but also many other countries in the world criticize other countries by name, including US President Biden demanding that Russian President Putin deter cyberattacks [74] [75].

Chapter 5 mentioned that the RTF, a ransomware attack countermeasure body, recommended that countries pressure other countries that were hiding attacker groups. In relation to this, the governments of countries that receive cyberattacks also need to show their stance to fight against cyberattacks. When an organization in your country receives a cyberattack, it not only damages that organization, but may also significantly affect the living and economic foundations of citizens, and further damage the entire nation. For this reason, attacked countries must demand that the other countries associated with attacker groups respond politically. It is believed that more countries will criticize such countries by name in the future.

It is also believed that such a trend will encourage state-sponsored attacker groups to further hide their identity information in order to prevent both themselves and the involved countries from being exposed. More specifically, it is speculated that they will try to prevent any trace of their attack from being analyzed, prevent their identity from being verified based on the remaining traces, pretend that another attacker group had made the attack, and so forth.

Cyberattacks if COVID-19 worsens again

As more people are getting vaccinated against COVID and the number of related deaths is also declining, the COVID pandemic may come to an end. On the other hand, the effectiveness of vaccination may deteriorate over time and the virus becomes more infectious in winter. As a result, COVID may worsen again, and vaccine booster shots may be required.

As people’s interest in the ongoing vaccination grew, many countries experienced phishing attacks exploiting information about the vaccines, including the theft of personal information and credit card information by spoofing vaccination booking sites [76] [77] [78]. If vaccine booster shots are required again, similar attacks will recur.

Cyberattacks after the pandemic

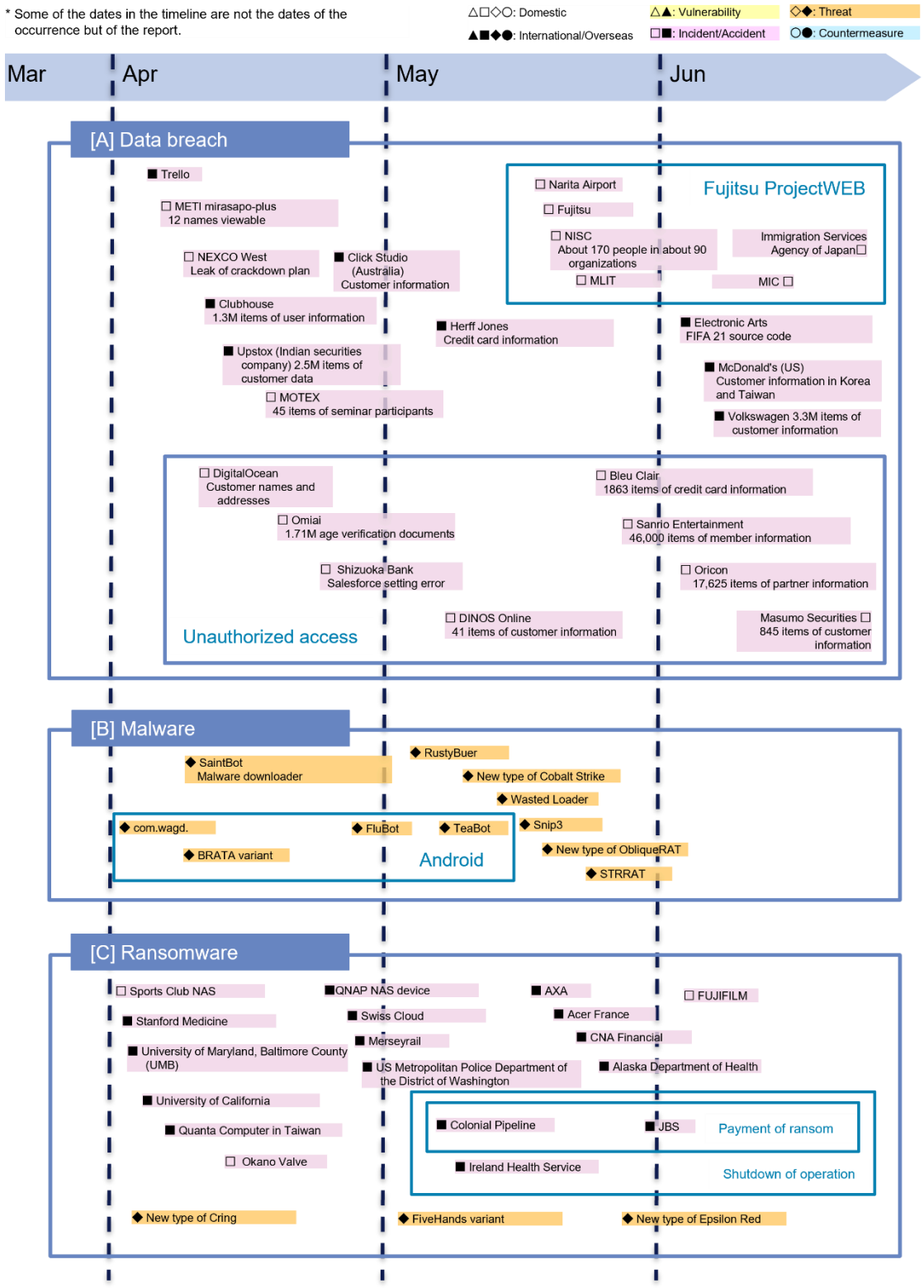
As more people are getting vaccinated against COVID and the number of related deaths is also declining, economic and leisure activities have started recovering in the world. If this trend continues, the targets of cyberattacks may shift from COVID-related events to wealthy industries in the post-COVID world. The following cyberattacks are expected to occur.

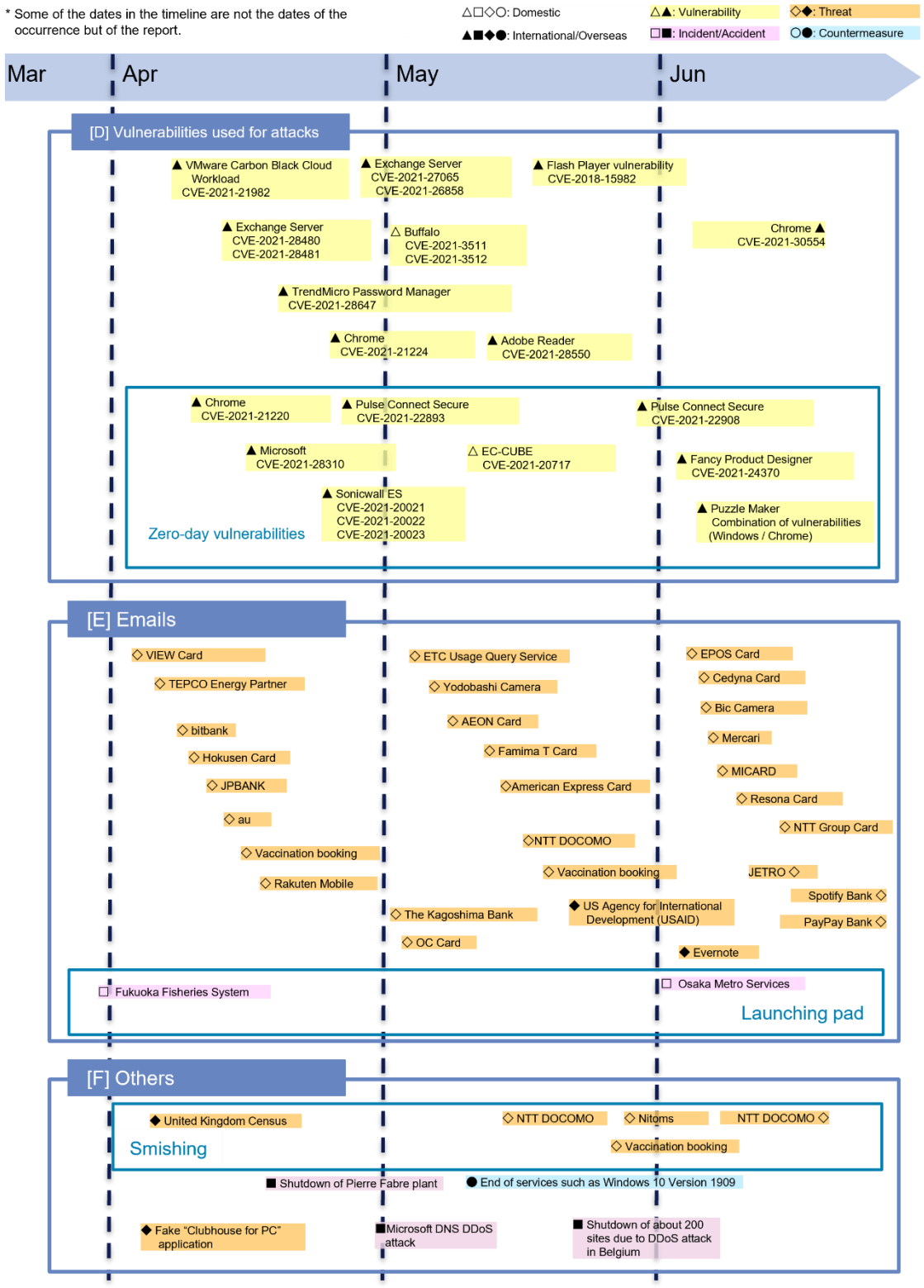
The first type of attack will target the pharmaceutical and healthcare industries. The pharmaceutical companies that have developed COVID vaccines are achieving higher performance due to increased sales. Since supplies of vaccines are stabilizing and the danger of COVID is becoming more controllable, it is predicted that attackers are likely to target pharmaceutical companies.

The second type of attacks are leisure-related phishing attacks. Those who have given up on fun events and travels due to COVID are desperate for leisure. Once people are released from pandemic restrictions in the post-COVID world, many will search for a wide range of leisure information on the Internet and make reservations to relieve their accumulated stress. Attackers will have an eye on that. There will be an increase in phishing emails and phishing sites related to leisure to trick leisure-hungry users.

The third type of attacks will target new businesses and investments that will become popular in response to economic recovery after the pandemic. Many investments are expected to be made in new businesses and companies recovering their business performance. Attackers will actively attack not only large companies, but also small-to-medium companies such as startups.

7. Timeline





References

[1] トレンドマイクロ株式会社, “Water Pamola Attacked Online Shops Via Malicious Orders,” 28 4 2021. [オンライン]. Available: https://www.trendmicro.com/en_us/research/21/d/water-pamola-attacked-online-shops-via-malicious-orders.html.

[2] “クレジットカード情報漏洩事件のまとめ（2021年上半期）,” 14 7 2021. [オンライン]. Available: https://foxestar.hatenablog.com/entry/2021/02/09/110000.

[3] 株式会社イーシーキューブ, “EC-CUBE 4.0系: クロスサイトスクリプティング脆弱性 (JVN#97554111) について,” 7 5 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210507/.

[4] 株式会社イーシーキューブ, “【重要】EC-CUBE 4.0系における緊急度「高」の脆弱性(JVN#97554111)発覚と対応のお願い,” 7 5 2021. [オンライン]. Available: https://www.ec-cube.net/news/detail.php?news_id=383.

[5] JPCERT/CC, “EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起,” 10 5 2021. [オンライン]. Available: https://www.jpcert.or.jp/at/2021/at210022.html.

[6] JVN, “JVN#97554111　EC-CUBE におけるクロスサイトスクリプティングの脆弱性,” 10 5 2021. [オンライン]. Available: https://jvn.jp/jp/JVN97554111/.

[7] 株式会社イーシーキューブ, “EC-CUBE3.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458),” 10 6 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210610/index30.php.

[8] 株式会社イーシーキューブ, “EC-CUBE4.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458),” 10 6 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210610/index40.php.

[9] JVN, “JVN#95292458　EC-CUBE における複数のクロスサイトスクリプティングの脆弱性,” 23 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN95292458/.

[10] JPCERT/CC, “複数のEC-CUBE 3.0系用プラグインにおけるクロスサイトスクリプティングの脆弱性に関する注意喚起,” 15 6 2021. [オンライン]. Available: https://www.jpcert.or.jp/at/2021/at210028.html.

[11] JVN, “JVN#79254445　複数の ETUNA 製 EC-CUBE 用プラグインにおけるクロスサイトスクリプティングの脆弱性,” 15 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN79254445/.

[12] JVN, “JVN#57524494　複数のイーシーキューブ製 EC-CUBE 用プラグインに

おける複数のクロスサイトスクリプティングの脆弱性," 15 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN57524494/.

[13] IPA, "「クロスサイト・スクリプティング（XSS）の脆弱性の種類」," [オンライン]. Available: https://www.ipa.go.jp/files/000024726.pdf.

[14] SSTバックヤード, "Stored(蓄積型)-XSSの危険性," 15 4 2020. [オンライン]. Available: https://techblog.securesky-tech.com/entry/2020/04/15/.

[15] JPCERT/CC, "ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃," 6 7 2021. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html.

[16] 株式会社イーシーキューブ, "セキュリティ対策について｜ご利用のEC-CUBEのバージョンを確認する," [オンライン]. Available: https://www.ec-cube.net/info/security/#securit_flow01.

[17] 株式会社イーシーキューブ, "EC-CUBE2・3・4系ダウンロード," 29 6 2021. [オンライン]. Available: https://www.ec-cube.net/download/other.php.

[18] "3.0系|配送伝票番号プラグイン(3.0系)|ETUNA," 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1001.

[19] "3.0系|配送伝票番号csv一括登録プラグイン(3.0系)|ETUNA," 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1007.

[20] "3.0系|配送伝票番号メールプラグイン(3.0系)|ETUNA," 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1089.

[21] 株式会社イーシーキューブ, "3.0系|帳票出力プラグイン|株式会社イーシーキューブ," 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=959.

[22] 株式会社イーシーキューブ, "3.0系|メルマガ管理プラグイン|株式会社イーシーキューブ," 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=960.

[23] 株式会社イーシーキューブ, "3.0系|カテゴリコンテンツプラグイン|株式会社イーシーキューブ," 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1070.

[24] 株式会社イーシーキューブ, "EC-CUBEプラグインをつくろう！ | ECサイト構築・リニューアルは「ECオープンプラットフォームEC-CUBE」," [オンライン]. Available: https://www.ec-cube.net/plugin/.

[25] EC-CUBE開発チーム, "html_entity_decodeを使っている箇所を修正," 15 6 2021. [オンライン]. Available: https://github.com/EC-CUBE/ProductReview-plugin/pull/71/files.

[26] 株式会社イーシーキューブ, “カテゴリコンテンツプラグイン バージョン1.0.1をリリースしました。,” 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/release/detail.php?release_id=5092.

[27] “「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について,” [オンライン]. Available: https://about.mercari.com/press/news/articles/20210521_incident_report/.

[28] “Bash Uploader Security Update,” [オンライン]. Available: https://about.codecov.io/security-update/.

[29] “【調査結果のご報告】「Codecov」への第三者からの不正アクセスによる 当社への影響および一部顧客情報等の流出について,” [オンライン]. Available: https://about.mercari.com/press/news/articles/20210806_incident_report/.

[30] “メルカリ、顧客情報など2万7千件流出　不正アクセスで,” [オンライン]. Available: https://www.asahi.com/articles/ASP5P6DCLP5PULFA02M.html.

[31] “グローバルセキュリティ動向四半期レポート2019 年度 第 1 四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_1q_securityreport.pdf.

[32] “メルカリを攻撃したcodecovのサプライチェーン攻撃の全貌：攻撃者のIPアドレスと攻撃者はどこの国？,” [オンライン]. Available: https://www.prsol.cc/?p=862.

[33] “グローバルセキュリティ動向四半期レポート2020 年度 第 3 四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[34] 株式会社日経新聞社, “婚活アプリ「Omiai」会員情報流出　最大171万,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUC21AEV0R20C21A5000000/.

[35] 株式会社朝日新聞社, “婚活アプリの個人情報が流出か　免許証など171万件,” [オンライン]. Available: https://digital.asahi.com/articles/ASP5P5Q3PP5PULFA02S.htm.

[36] SBクリエイティ株式会社, “eKYCとは何か？ 本人確認や銀行口座連携の手法、関連サービスを解説,” [オンライン]. Available: https://www.sbbit.jp/article/fj/46184.

[37] 経済産業省, “オンラインサービスにおける身元確認手法の整理に関する検討報告書,” [オンライン]. Available: https://www.meti.go.jp/press/2020/04/20200417002/20200417002-3.pdf.

[38] 金融庁, “オンラインで完結する自然人の本人特定事項の確認方法の追加,” [オン

ライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181130/01.pdf.

[39] 金融庁, “犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概,” [オンライン]. Available: https://www.fsa.go.jp/common/law/guide/kakunin-qa/2.pdf.

[40] 鈴. 淳也, “マイナンバーカードとJPKIで本人確認の仕組みは普及するか,” [オンライン]. Available: https://www.watch.impress.co.jp/docs/series/suzukij/1313080.html.

[41] 警察庁, “犯罪統計,” [オンライン]. Available: https://www.npa.go.jp/publications/statistics/sousa/statistics.html.

[42] 株式会社TIプランニング, “顔写真の自動照合機能を搭載したIC免許証の本人確認パッケージ（NEC）,” [オンライン]. Available: https://paymentnavi.com/cardnavi/19152.html.

[43] TRUSTDOCK, “eKYC身分証アプリ「TRUSTDOCK」にて、三菱UFJ銀行の「本人確認サポート（個人） APIサービス」との連携による、犯収法eKYC[ト1]の提供を今夏より開始。顔写真が不要なeKYCが可能に。,” [オンライン]. Available: https://prtimes.jp/main/html/rd/p/000000066.000033766.html.

[44] 総務省, “公的個人認証サービスの利活用について,” [オンライン]. Available: https://www.soumu.go.jp/main_content/000324414.pdf.

[45] M. Vanhoef, “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation,” [オンライン]. Available: https://papers.mathyvanhoef.com/usenix2021.pdf.

[46] ASCII.jp, “無線LAN規格「IEEE802.11」について知ろう,” [オンライン]. Available: https://ascii.jp/elem/000/000/455/455925/.

[47] M. Vanhoef, “FragAttacks,” [オンライン]. Available: https://www.fragattacks.com/.

[48] 永. 健. 康. 健. 泰司, “IEEE802.11とWi-Fi Allianceにおける 無線LANの標準化動向,” [オンライン]. Available: https://www.ntt.co.jp/journal/1002/files/jn201002077.pdf.

[49] TechTarget, “Wi-Fiデバイスのほぼ全てに影響　無線LANの脆弱性「FragAttacks」とは？,” [オンライン]. Available: https://techtarget.itmedia.co.jp/tt/news/2106/19/news01.html.

[50] M. Vanhoef, “FragAttacks: Presentation at USENIX security’21,” [オンライン]. Available: https://www.youtube.com/watch?v=OJ9nFeuitIU.

[51] ICASI, “Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on Aggregation and Fragmentation Attacks against Wi-Fi,” [オンライン]. Available: https://www.icasi.org/aggregation-fragmentation-attacks-

against-wifi/.

[52] NIST, “NVD - Search and Statistics - National Vulnerability Database,” [オンライン]. Available: https://nvd.nist.gov/vuln/search.

[53] Japan Vulnerability Notes, “JVNVU#93485736　IEEE802.11 規格のフレームアグリゲーションやフラグメンテーションに関する複数の問題（FragAttack）,” [オンライン]. Available: https://jvn.jp/vu/JVNVU93485736/.

[54] Wi-Fi Alliance, “Wi-Fi Alliance® security update – May 11, 2021 | Wi-Fi Alliance,” [オンライン]. Available: https://www.wi-fi.org/security-update-fragmentation.

[55] Bloomberg, “Colonial Hackers Stole Data Thursday Ahead of Shutdown,” 9 5 2021. [オンライン]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

[56] BBC NEWS JAPAN, “世界最大の食肉加工会社にサイバー攻撃、米豪の工場が停止　ロシアの犯罪集団関与か,” 2 6 2021. [オンライン]. Available: https://www.bbc.com/japanese/57325741.

[57] 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年度版　第3四半期）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[58] THE WALL STREET JOURNAL, “Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom,” 19 5 2021. [オンライン]. Available: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

[59] CNN, “Colonial Pipeline CEO defends his handling of ransomware attack that crippled East Coast fuel supply,” [オンライン]. Available: https://edition.cnn.com/2021/06/08/politics/colonial-pipeline-ceo-on-capitol-hill-ransomware/index.html. [アクセス日: 8 6 2021].

[60] BBC NEWS JAPAN, “サイバー被害の米パイプライン、身代金の大半を回収　米司法省が発表,” 8 6 2021. [オンライン]. Available: https://www.bbc.com/japanese/57394900.

[61] REUTERS, “米コロニアル・パイプラインのハッカー、大量のデータを窃盗＝ＢＢＧ,” 9 5 2021. [オンライン]. Available: https://jp.reuters.com/article/usa-products-colonial-pipeline-idJPKBN2CQ03O.

[62] JAFIC, “マネーロンダリング対策の沿革,” [オンライン]. Available: https://www.npa.go.jp/sosikihanzai/jafic/maneron/manetop.htm. [アクセス日: 21 7 2021].

[63] Yahoo! ニュース, “FBIはどうやってハッカーから身代金を取り戻したのか,” 11

6 2021. [オンライン]. Available: https://news.yahoo.co.jp/articles/3d24553a6e171339e9e88388746d1271982bc19e.

[64] npr, “How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back,” 8 6 2021. [オンライン]. Available: https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac.

[65] CNBC, “The FBI likely exploited sloppy password storage to seize Colonial Pipeline bitcoin ransom,” 9 6 2021. [オンライン]. Available: https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html.

[66] “Seizure Warrant,” [オンライン]. Available: https://www.scribd.com/document/510927692/Seizure-Warrant#download&from_embed.

[67] THE UNITED STATES DEPARTMENT of JUSTICE, “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” 7 6 2021. [オンライン]. Available: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[68] Institute for SECURITY+TECHNOLOGY, “RANSOMWARE TASK FORCE,” [オンライン]. Available: https://securityandtechnology.org/ransomwaretaskforce/. [アクセス日: 20 7 2021].

[69] Institute for SECURITY+TECHNOLOGY, “RTF Report: Combatting Ransomware,” [オンライン]. Available: https://securityandtechnology.org/ransomwaretaskforce/report/. [アクセス日: 20 7 2021].

[70] 朝日新聞, “警察庁がサイバー局を新設へ　自ら捜査する「直轄隊」も,” 24 6 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP6S3DBNP6RUTIL06J.html.

[71] NHK, “警察庁「サイバー局」新設へ 重大なサイバー犯罪の独自捜査も,” 24 6 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210624/k10013101201000.html.

[72] 朝日新聞, “警察庁、対サイバー体制強化　局新設方針／自ら捜査へ直轄隊,” 25 6 2021. [オンライン]. Available: https://www.asahi.com/articles/DA3S14950563.html?pn=3.

[73] NHK, “JAXAなどに大規模なサイバー攻撃 中国人民解放軍の指示か,” [オンライン]. Available:

https://www3.nhk.or.jp/news/html/20210420/k10012984761000.html. [アクセス日: 20 4 2021].

[74] 産経新聞, “米露首脳が電話会談　バイデン氏サイバー攻撃阻止要求,” 10 7 2021. [オンライン]. Available: https://www.sankei.com/article/20210710-BYXSB5KZ2ZMGHMGE67UURCDMCA/.

[75] REUTERS, “ノルウェー議会へのサイバー攻撃、中国が発信源＝外相,” 19 7 2021. [オンライン]. Available: https://jp.reuters.com/article/norway-cyber-idJPKBN2EP1GO.

[76] FEDERAL BUREAU OF INVESTIGATION, “Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines,” FEDERAL BUREAU OF INVESTIGATION, 20 12 2020. [オンライン]. Available: https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines.

[77] BBC., “Beware fake Covid vaccination invites, NHS warns,” BBC., 26 1 2021. [オンライン]. Available: https://www.bbc.com/news/technology-55811161.

[78] 宇. 充, “新型コロナワクチン関連のフィッシング詐欺に要注意。防衛省や厚労省が呼びかけ,” 株式会社インプレス Impress Corporation, 31 8 2021. [オンライン]. Available: https://pc.watch.impress.co.jp/docs/news/1347158.html.

[79] 経済産業省, “株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）,” 20 12 2019. [オンライン]. Available: https://www.meti.go.jp/press/2019/12/20191220013/20191220013.html.

[80] IPA, “ECサイト構築で多く利用されている「EC-CUBE」を用いたウェブサイトでの情報漏えい被害の増加について,” 25 12 2019. [オンライン]. Available: https://www.ipa.go.jp/security/announce/alert20191225.html.

[81] 情報処理推進機構, “情報セキュリティ　10大脅威 2021,” 2 2021. [オンライン]. Available: https://www.ipa.go.jp/files/000088835.pdf.

[82] 国土交通省, “令和２年度　テレワーク人口実態調査　－調査結果の抜粋－,” 3 2021. [オンライン]. Available: https://www.mlit.go.jp/report/press/content/001391381.pdf.

[83] 総務省, “サイバー攻撃の最近の動向等について,” 3 12 2020. [オンライン]. Available: https://www.soumu.go.jp/main_content/000722477.pdf.

[84] 朝日新聞DIGITAL, “三菱電機へのサイバー攻撃、VPN装置にハッキングか,” 2 5 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN517HP7N4XULZU012.html.

[85] 朝日新聞DIGITAL, “狙われた、社内への「接続口」　三菱電機へのサイバー攻

撃、ＶＰＮ経由か,” 8 5 2020. [オンライン]. Available: https://www.asahi.com/articles/DA3S14468115.html.

[86] cnet Japan, “世界中で医療機関へのサイバー攻撃が頻発、2020年11月に45%増--ランサムウェア多用,” 8 1 2021. [オンライン]. Available: https://japan.cnet.com/article/35164749/#:~:text=%E5%8C%BB%E7%99%82%E9%96%A2%E4%BF%82%E6%A9%9F%E9%96%A2%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E3%81%AE%E5%A2%97%E5%8A%A0%E7%8E%87%E3%82%92%E5%9C%B0%E5%9F%9.

[87] FBI, “FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic,” 21 3 2021. [オンライン]. Available: https://www.ic3.gov/Media/Y2020/PSA200320.

[88] FBI, “FBI Urges Vigilance During COVID-19 Pandemic,” [オンライン]. Available: https://www.fbi.gov/coronavirus.

NTT DATA
Trusted Global Innovator

Published on November 2, 2021

NTT DATA Corporation
Security Engineering Department
Hisamichi Ohtani / Chihiro Ohyama / Kunio Miyamoto / Mao Ohishi / Kenshiro Itayama / Kazuho Oh / Daisuke Miyazaki / Misumi Nakamichi / Masazumi Ohyama / Yuji Kamiya / Toshihiko Sasaki / Mika Takita
nttdata-cert@kits.nttdata.co.jp