Quarterly Report on Global Security Trends

3rd Quarter of 2023

Table of Contents

1. Executive Summary

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

New style My Number cards

The Japanese Government announced that My Number cards will be revamped and new-style cards will be introduced in 2026. Due to the occurrence of card counterfeiting cases, it has been discussed not to have the information printed on the card surface and instead to record the content in the IC chip on the My Number card. As a result of considering visual or image data-based identity verification operations, however, it was decided to keep the address, name, date of birth, and facial photo information.

While the penetration of the IC chip reading environment remains low, it is likely a similar situation will continue. Therefore, attention is required in handling the information at the visual verification sites.

Is multi-factor authentication sufficient? Recommending Passkey

Password-less authentication “Passkey” is a multi-factor authentication system that can resolve the issues of conventional multi-factor authentication and has the advantage of further enhancing both security and usability.

With increased support from major platforms, Passkey is increasingly becoming a “new standard”. It is essential for organizations to adapt to this change to maintain competitiveness. For this reason, organizations’ information system personnel are recommended to actively evaluate and consider implementing Passkey.

Importance and effectiveness of information sharing in the event of a security incident

In recent years, there has been increased movement toward requiring information sharing in the event of a security incident in various countries. In Japan, in contrast, information sharing in the event of a security incident has not always been progressive.

In many cases, organizations that have suffered from cyberattacks tend to be cautious about information disclosure, thinking that disclosure of detailed information about the security incident would negatively affect their reputation. It is considered desirable to appropriately share information, by utilizing the “Guidance for Sharing and Publication of Information on Damage from Cyberattacks”, to maximize the benefits of both the own organization and the whole of society.

Continuing exploitation of serious vulnerabilities in Citrix products

The overview of “CVE-2023-3519”, a zero-day vulnerability in Citrix products, attack methods and countermeasures, and actual incident response and vulnerability response cases and the lessons learned in these cases are provided here in an organized manner.

There is a recognition that zero-day vulnerabilities rarely occur, only in irregular cases. It is found, however, there were many cases of zero-day vulnerabilities and the damage they caused were announced in FY2023, and the number is increasing. To protect the organization from damage from cyberattacks, it is important to correctly understand zero-day vulnerabilities and to make the necessary responses.

Future ransomware attack methods, considering the emergence of no-ware ransom

Ransomware called “no-ware ransom” that does not encrypt files has emerged.

With the increasing number of organizations that implement data backup measures, etc., it is assumed that the number of cases of damage from conventional ransomware attacks will level off, while it is assumed that the number of no-ware ransom attacks that steal data will increase. In addition, since technical support from criminal organizations becomes easier for reasons such as decryption being not required, it is assumed that the supply of the RaaS version of no-ware ransom will also increase, as will the damage from it.

2. Featured Topic “new style My Number cards”

Yuto Kihira, Cyber Security Department, NTT DATA Group

2.1. Changes in new style My Number cards

The Japanese Government made a cabinet decision on the “Priority Plan for Realizing a Digital Society” in June 2023 [1]. As part of the Plan, it was announced that the current My Number cards which have been issued since 2016 will be revamped and new style cards will be introduced in 2026. Since the expiration date of the current My Number cards is approximately 10 years until the 10th birthday from the date of issuance, new style My Number cards will be introduced to coincide with the deadline for renewal for those who began using their My Number cards immediately after the cards were issued. With the aim of considering the matters that contribute to the functional improvement of these new style cards, the “Task Force for Next Personal Number Cards” was established in September 2023 [2]. This Task Force decided on changes to the next cards and published the interim summary in December 2023 [3].

Although the changes to the next My Number cards are wide-ranging, the most beneficial change for users is to extend the expiration date of the electronic certificates of the My Number cards from five to ten years. With the current My Number cards, the expiration date of electronic certificates is five years while that of the card itself is ten years. For this reason, users need to visit municipal offices to renew electronic certificates when five years have passed since the issuance, posing a burden on users. Therefore, by extending the expiration date of electronic certificates to approximately ten years, the same as that for the My Number card, the renewal procedure required in the fifth year will no longer be required, thereby reducing the burden on users.

In conjunction with this, the encryption method will also be reviewed. For RSA 2048bit used for the current My Number cards, the deadline for its use is set at 2030 in the e-Government Recommended Ciphers List (CRYPTREC) [4]. With the next My Number cards, for which the expiration date of electronic certificates will be approximately 10 years from the issuance, RSA 2048bit cannot continue to be used as the deadline for its use will be exceeded. Therefore, for the public key encryption method for the next My Number cards, ECDSA 256bit and ECDSA 384bit will be adopted as robust public key encryption methods that can be used until 2036.

In addition to these, the design and the information printed on the My Number card surface will also be changed. Although the specific design has not been published yet, the surface design is planned to be reviewed based on anti-counterfeiting, universal design support, and consideration for people with visual disabilities, etc. It has been announced that particular consideration will be given to the ease of reading the text and attractive design, so the card will be one that everyone will want to own. In addition, of the four basic pieces of information, namely the address, name, gender, and date of birth, and the face photo printed on the current My Number card surface, gender will be removed from the next My Number card surface. Furthermore, the furigana for the name will be added, and for those who have requested, the date of birth in the Western calendar year and the name in English characters will be printed in the additional field. Many changes other than the above will also be made to the next My Number cards.

2.2. Occurrence of counterfeiting cases

During the period when the Task Force for Next Personal Number Cards

published the interim summary, there was another new My Number card-related report of note. It was a news report covering the first arrest for My Number card counterfeiting [5]. The suspect counterfeited My Number cards based on the face photo, address, and other data sent from the suspect's superior in China and then sent them to men and women of Vietnamese, Indonesian, and other nationalities. The counterfeit My Number cards are assumed to have been used as official identification cards for in-person identity verification when opening bank accounts and signing mobile phone contracts. Those bank accounts and mobile phones are assumed to be used for crimes such as phone fraud.

The counterfeit My Number cards were created with an IC chip embedded to make them look like the real ones, but other various anti-counterfeiting and alteration measures applied to the real My Number cards were not applied. As a result, they were far from elaborate counterfeits. It is extremely difficult to duplicate/counterfeit digital certificates stored in the IC chip. Therefore, the IC chips were only for appearance and did not contain any information. For this reason, the counterfeit My Number cards used in this case cannot be used to impersonate a real individual to log in to the My Number portal or use e-tax to submit electronic documents, which require authentication using the IC chip embedded in the card. Such IC chip-based authentication uses two types of electronic certificates stored in the IC chip, namely the electronic certificate for user verification and that for the signature. The authentication method using these electronic certificates is completely different from the currently most widely used authentication based on ID and password. Duplicating/counterfeiting these certificates stored in the IC chip is extremely difficult, and it is impossible to break through authentication using these certificates with the counterfeit cards used in this case, which counterfeited the card surface only.

However, My Number cards can be used as an identity verification document with a face photo along with a driver's license or passport for in-person identity verification in most cases. There are also operations in which identity verification is performed by attaching a copy of the My Number card to a document and mailing it. In such cases, the information in the IC chip is not read and the identity verification is based only on visual inspection of the card surface. In the operations in which the information in the IC chip is used for identity verification, counterfeiting is readily recognized. In the verification based on visual inspection of the card surface only, in contrast, counterfeit determination relies solely on visual information and there will be a risk of overlooking. If a bank teller overlooks counterfeiting, a fake bank account can be opened and used for criminal acts. To prevent such situations, strict identity verification is important. Therefore, it is recommended to perform identity verification by not solely relying on the human eye, but also using the information in the IC chip in combination.

2.3. Information printed on the card surface

In the Task Force for Next Personal Number Cards [3], because of a risk of data breach in the event of theft or loss, etc., it was discussed for the next My Number cards not to have the basic four pieces of information and face photo printed on the front side and the My Number on the back side, and instead to record them in the IC chip equipped on the My Number card. As a result of considering the fact that the environment for reading the data in the IC chip is not available at all identity verification sites at present and that the operations of identity verification by visual inspection of the card surface and copying of the card surface are unlikely to go away anytime soon, however, it was decided to continue to have the address, name, date of birth, and face photo printed on the card surface. In addition, when the respective agencies have the owner of the My Number card submit his/her My Number card, they will refer to the My Number printed on the My Number card because the environment for reading the data in the IC chip is also not yet available near at hand. In consideration of this, it was also decided to continue to have the My Number information printed on the back side as with the current cards. On the other hand, based on the

judgment that there are not many occasions when visual inspection of the gender information is required in in-person identity verification, it was decided not to have the gender information printed on the card surface and have that information only recorded in the IC chip. As a result of determining the information to be printed on the card surface with consideration given to the My Number card usage status on site, for the next My Number card, the risk of data breach and counterfeiting remains unchanged from the current ones. In addition, with the information provision methods using the card surface of the My Number card, it is difficult to select and submit only the required information, such as name only or date of birth (age) only, from among the personal attribute information. For this reason, those who submit their My Number cards and those who receive them both have privacy concerns that unnecessary information may be submitted/obtained.

2.4. Outlook for the next and subsequent My Number cards

According to the interim summary published by the Task Force for Next Personal Number Cards, My Number cards will continue to be improved in the future. When considering the risk of personal data breach, the goal of My Number cards should be not to have any personal information printed on the card surface and to perform identity verification using the data in the IC chip. Due to the reasons given above, however, for the next My Number cards, only the gender information will be removed from the card's surface. Considering the above, to achieve the ideal form of the My Number cards, it is necessary to lower the barriers to reading the IC chip of the My Number cards for both business operators performing identity verification and users presenting identify information.

To perform identity verification using the IC chip, business operators must have a device to read the IC chip and a mechanism to verify the validity of the content. They also need to review the operation of copying the card surface remaining on site. This cannot be achieved overnight. Therefore, to improve the current situation as much as possible, the Government's policy is to develop and distribute for free an app that can read the basic four pieces of information, including gender, and the My Number from the IC chip through smartphones, etc. With this, it may be possible to convert company smartphones directly into devices for reading the IC chip, eliminating the need for installing dedicated equipment for reading and verifying the IC chip.

As for users, discussions are underway on the ways to reduce the burden of identity authentication by using the IC chip. Reviewing the PIN code is one of them. The current My Number cards contain four apps: JPKI app, basic resident register app, card surface information verification app, and card surface information entry assistance app, and different PIN codes can be set for each of them. The same PIN code can be set for these apps excluding the JPKI app. However, it is difficult for general users to enter the correct PIN code by identifying the app to be used from among the four apps when prompted by the service to read the IC chip and enter the PIN code. There is also an issue that when a service uses multiple apps, it is necessary to enter the PIN code corresponding to the respective apps, which can be a cumbersome operation. In response to these issues, for the next My Number cards, discussions are ongoing to integrate the PIN codes into two PIN codes, a 6- to 16-digit PIN code for the signature and a 4-digit PIN code for other purposes, and not to require the verification of the 4-digit PIN code when the verification of the PIN code for the signature is successful. In addition, installation of the JPKI app on Android smartphones has been achieved to date. iPhone support and installation of apps other than the JPKI app will be promoted in the future, and discussions will be made to achieve an authentication method with less user burden such as biometric authentication, rather than PIN code-based authentication.

To achieve the ideal form of not having personal information printed on the card surface, various efforts are being discussed as described above. It is expected to take some time, however, until the IC chip reading environment

becomes available in all the identity verification sites. Discussions need to be continued on the level of availability that can be deemed sufficient to remove the personal information from the card surface and what efforts should be made in the future. In addition, even with the level of availability becoming sufficiently high, the matters to be considered are wide-ranging, including operations in abnormal situations such as in the event of a disaster. Measures to address these issues also need to be considered. At present, Japan is approaching the ideal form of a digital society through various initiatives. Removal of personal information from the My Number card surface is only one aspect of such initiatives, but we hope that steady progress will be made to achieve it.

3. Featured Topic “Is multi-factor authentication sufficient? Recommending Passkey”

Hidehito Hodoyoshi, Cyber Security Department, NTT DATA Group

Password-less authentication “Passkey” addressed in the Quarterly Report on Global Security Trends 3rd Quarter of 2022 is a type of multi-factor authentication that can significantly enhance security and improve usability at the same time. As projected in the Quarterly Report, it has been implemented in more and more domestic services [5].

The steps and precautions for implementation while mentioning the situation and basic concepts, etc., of the Passkey are presented here.

3.1. Environment for implementing Passkey is ready

Implementation and prevalence of Passkey began in the second half of 2022 when it was supported by some platforms (Apple, Google). In 2023, Windows also started supporting Passkey, making it available on major platforms. Furthermore, password management services such as 1Password and LastPass, etc., also supported Passkey, which allowed the use of Passkey in a cross-platform environment. To allow users to log in easily and securely, many services, including Adobe, Amazon, Apple, CVSHealth, Dashlane, DocuSign, Google, Mercari, NTT DOCOMO, and Nintendo, began providing Passkey [6]. Expanded support for Passkey by major platforms means that the adoption and provision of Passkey will become even easier in the future.

Such development of Passkey has important implications for companies’ information system personnel. By adopting advanced security technologies such as Passkey, companies can simplify the process for employees to log in to the information system and improve safety.

3.2. Explanation on Passkey

3.2.1. Basic concept and operating principle of Passkey

Passkey is a new password-less authentication method designed to provide greater security and usability than conventional password-less authentication methods. Passkey uses public key encryption technology and performs authentication using two keys: a public key and a private key. Public keys are registered with the information system, and private keys, which should be kept confidential, are stored only on the users’ devices.

In the authentication process using Passkey, when a user enters an account ID to log in to the information system, the information system sends an authentication request to the device, such as a PC or smartphone, used by that user. The device uses the private key to sign the request. The device then returns the signed request to the information system, and the service provider verifies the signature using the public key. If the verification of the signature succeeds, it is proved that the user is the legitimate owner of the account and the login to the system is therefore allowed.

An important point of Passkey is that the private key exists only on the user’s device and is never sent outside the user’s device. This can prevent the risk of

password leakage resulting from users falling for phishing attacks. Therefore, authentication security is enhanced significantly.

3.2.2. Characteristic 1: Robust security

Authentication using Passkey is an authentication method based on public key encryption technology. Since the public key is stored only on the user's device and next sent outside that device, the risk of private key leakage is extremely low. In the authentication process, the private key is used to sign a request and the signature is verified by the service provider. This process significantly reduces the risk of unauthorized access and data breach, thereby providing robust security for companies and users.

3.2.3. Characteristic 2: Enhanced usability

Passkey provides a significant improvement in usability. In place of a conventional password-based or complex multi-factor authentication process, Passkey allows users to easily complete authentication using device biometrics or PINs. This simple and intuitive approach speeds up the login process and contributes to enhanced usability.

Multi-factor authentication can improve the strength of authentication, but in return reduces usability during authentication. For instance, methods that receive an authentication code via SMS or methods that use physical tokens require additional time and effort in the authentication process for users. As described above, multi-factor authentication has a tradeoff between usability and security.

In contrast to multi-factor authentication, Passkey does not require additional time and effort in the authentication process or additional security measures such as physical tokens. Since authentication can be completed simply with biometric authentication using the user's device when accessing the information system, usability can be improved significantly. As just described, Passkey is a new authentication method that significantly improves the usability of multi-factor authentication.

3.2.4. Characteristic 3: Resistance to phishing attacks

Passkey-based authentication has strong resistance to theft of authentication information and attack methods that steal and exploit authentication information, such as phishing, in particular.

The reason that Passkey is suitable for recent security environments resides in its fundamental security structure.

First, it uses device biometrics in place of passwords to significantly reduce the attack vector that attackers can use. Next, in this authentication method, the authentication process is completed entirely within the device without requiring the user to provide his/her private key information to the service provider, making it difficult for attackers to steal authentication information via phishing sites. Passkey stores private keys safely on the users' devices and performs authentication through public keys, thus making it difficult for attackers to steal users' authentication information. In addition, the Passkey-based authentication process only authenticates requests from legitimate service providers and can therefore effectively eliminate fake authentication requests.

As described above, Passkey has been a powerful tool to counter security threats targeting authentication information such as phishing attacks in recent years, and can be a key for companies to effectively achieve a balance between security and usability.

3.2.5. Comparison between Passkey and multi-factor authentication

There are some important differences between Passkey and multi-factor

authentication.

Multi-factor authentication performs authentication by combining multiple authentication factors based on knowledge information such as passwords, possession information such as devices, and biometric information such as fingerprints for enhanced security. While there is only one authentication barrier that attackers must overcome for authentication solely relying on passwords, multi-factor authentication provides multiple barriers against unauthorized access. Multi-factor authentication can improve the strength of authentication, but in return reduces usability during authentication as it requires multiple authentication operations from a user as shown as Issue (1) in Figure 3-1. In other words, there is a tradeoff between usability and security. In addition, multi-factor authentication has vulnerabilities shown as Issues (2) and (3) in Figure 3-1. For instance, attackers may be able to steal IDs, passwords, and other information through phishing and password spray, etc., by targeting this vulnerability. Attackers can break through authentication by swapping the SIM for the attacker's SIM using the IDs and passwords they stole.

In contrast to multi-factor authentication, Passkey does not require adding authentication processes or additional devices such as physical tokens, and can be completed simply with biometric authentication using the user's device when accessing the information system. Therefore, authentication can be done in a single operation as shown as Solution (1) in Figure 3-1, thus significantly improving the usability. Furthermore, as shown as Solutions (2) and (3) in Figure 3-1, Passkey performs authentication by sending the authentication result without using authentication information such as the password, and uses robust public key encryption technology to provide resistance to phishing and password list attacks.

As just described, Passkey is a new authentication method that is safer and provides more improved usability than multi-factor authentication.

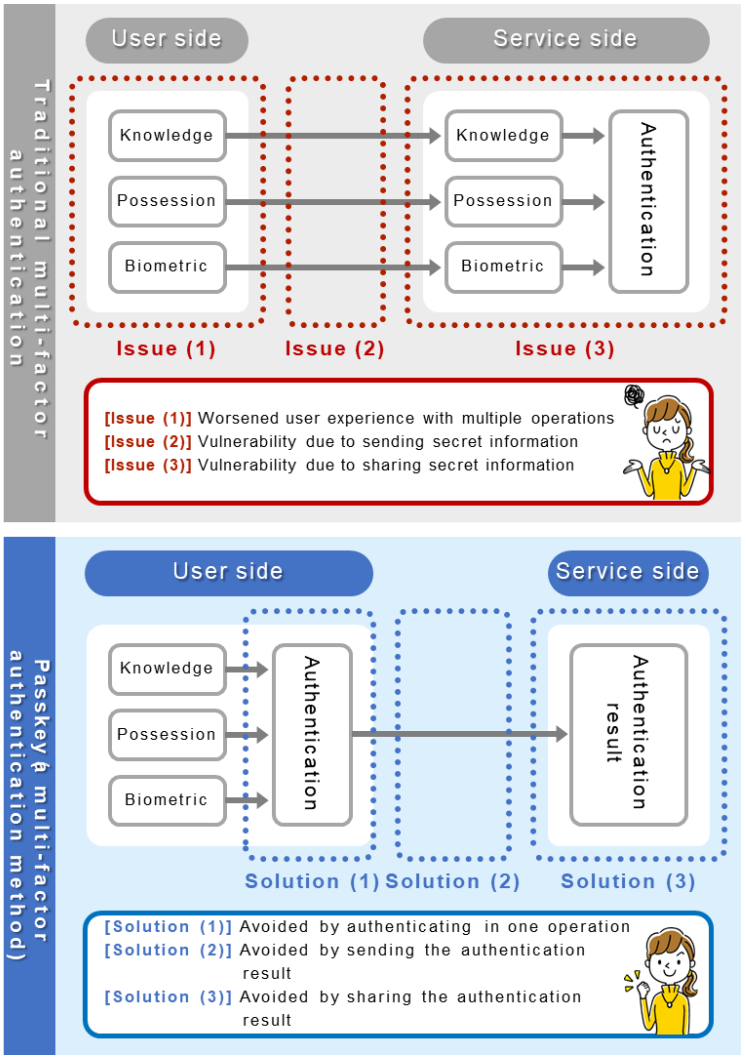


Figure 3-1 Comparison between multi-factor authentication and Passkey

3.3. Implementation and operation of Passkey

3.3.1. Steps for implementation

Passkey can easily be implemented as many new systems, including as online services, mobile applications, and cloud-based services, support FIDO authentication. Passkey is a mechanism to provide authentication using user devices, and is therefore suitable to be implemented in information systems requiring personal authentication, including an OA environment and remote work environment.

On the other hand, it cannot be implemented in information systems that do not identify individuals during authentication or information systems in which a single account is used by multiple users such as shared PCs. In addition, since it requires a means to send an authentication request from the user's device to the information system, it is also not suitable to be implemented in information systems that are not connected to the Internet.

Therefore, when implementing in the information system, the first step is to evaluate the compatibility of Passkey with the current authentication system to identify required system updates and changes for supporting Passkey. The next step is to select the technology required for design and implementation with an appropriate Passkey product vendor and formulate a Passkey implementation plan that meets the system needs. In the implementation step, not only technical matters, but also education and training for employees will be required. It is also necessary to provide guidance to enable employees to understand the concepts and how to use Passkey and be able to use Passkey safely. The last step is to establish the policy and procedures to support Passkey operations and implement appropriate security audit and reporting mechanisms.

3.3.2. Considerations during implementation and operation

There are some considerations when implementing and operating Passkey.

3.3.2.1. Compatibility

If the devices used by users, such as PCs and smartphones, are not standardized within the company, users can use a PC, smartphone, and operating system of their preference. Therefore, the information system personnel must consider the compatibility with all those devices and operation systems, and secure knowledge and structure to broadly support various devices and operating systems.

It is necessary to examine and compare benefits and costs, and if needed, take measures to limit the types of PCs, smartphones, and other devices that users use, etc.

3.3.2.2. Support

In Passkey-based authentication, the information required for authentication is stored on the user's device. Therefore, when compared to conventional password-based authentication, the authentication recovery process may become complex when the user's device fails, is lost, or is replaced with a new device. For this reason, the recovery process needs to be examined in detail.

3.3.2.3. Rules, etc.

Information systems using Passkey, including user devices, (but not exclusively) must comply with laws and regulations concerning safety and privacy of user data, security policies, privacy requirements, and industrial best practices, etc. It is necessary to ensure that the highest priority is given to safety and privacy of user data and that laws and regulations, etc., are strictly observed.

3.4. Conclusion

Passkey is a new authentication method that plays an important role in the recent security environment. The use of Passkey has advantages of resolving the issues of multi-factor authentication and enhancing both security and usability.

In addition, in recent years, attention has been drawn to incidents in which attackers attack the target companies by hacking into their business partners or group companies and impersonating users of those companies. In consideration of such supply chain security risks, customers and parent companies are requesting organizations in the supply chain to enhance their user authentication security measures. Given this background, companies implementing Passkey in their information systems means more than just adopting the latest authentication methods. Implementing Passkey is a strategic decision to gain customer trust and maintain competitiveness within the industry. Companies that have implemented Passkey are realizing the benefits of adopting Passkey.

Passkey is also increasingly becoming a “new standard” with more and more major platforms supporting it. It is essential for companies to adapt to this change to maintain competitiveness. For this reason, information system personnel are recommended to actively evaluate and consider implementing Passkey.

4. Data breach “Importance and effectiveness of information sharing in the event of a security incident”

Reiko Tasugi / Akira Takeda
Cyber Security Department, NTT DATA Group

On August 4, 2023, three organizations, namely the National Center of Incident Readiness and Strategy for Cybersecurity (hereinafter “NISC”), Meteorological Agency, and Meteorological Research Institute, announced that a part of email data containing personal information may have been leaked outside due to unauthorized communication to email-related equipment. This section presents the post-incident response to the above and provides an opinion on whether an incident report is required.

4.1. Movement for sharing information on security incidents in respective countries

In recent years, there has been increased movement toward requiring information sharing in the event of a security incident in various countries.

In the U.S., the Securities and Exchange Commission (SEC) started applying the cybersecurity disclosure rules to listed companies in the U.S. market in December 2023 [7]. The cybersecurity disclosure rules require listed companies to report important matters that affect the financial conditions and/or stock prices using the report form “Form 8-K” within four days of discovering a security incident and determining that the damage is significant.

In Europe, on the other hand, the European Cyber Resilience Act [8] is currently being considered. This Act imposes various security measures on products with digital elements. The manufacturers and developers are required to report within 24 hours when a vulnerability is discovered or the occurrence of a security incident is detected.

In Japan, starting from April 2022, it is required by the revised Act on the Protection of Personal Information to report to the Personal Information Protection Commission when a leakage of personal information, etc., occurs and there is a risk of harm to the rights and interests of individuals [9]. On the other hand, there is no obligation to report the occurrence of other security incidents, but the “Matters to Be Addressed Promptly to Strengthen Japan’s Cybersecurity [Urgent Recommendations]” [10] compiled by the Ministry of Internal Affairs and Communications requires prompt information sharing on the security incident.

There are several reasons for recommending information sharing in the event of a security incident. The first reason is ensuring the transparency of the status of damage related to the incident for investors as required by the SEC’s cybersecurity disclosure rules. The second reason is protection of victims and public interests as required by the European Cyber Resilience Act and the Ministry of Internal Affairs and Communications. In Japan, however, information sharing in the event of a security incident has not always been progressive. The

post-incident response to the email data leakage incidents of the NISC, Meteorological Agency, and Meteorological Research Institute is discussed here.

4.2. Email data leakage incidents of the three organizations

(1) Overview of the security incident of the NISC

On June 13, 2023, traces of unauthorized communication were found in the NISC's email-related system/equipment. To investigate the situation, NISC promptly suspended the operations of the affected system. NISC then replaced the email-related equipment and after confirming that there were no abnormalities in other equipment, restarted the system concerned. Later, from the results of the investigation by an external security-specialized agency, it was discovered that a part of email data containing personal information received from outside NISC during the period from early October 2022 to mid-June 2023 may have been leaked outside [11].

(2) Overview of the security incidents of the Meteorological Agency and Meteorological Research Institute

The Meteorological Agency and Meteorological Research Institute announced, respectively, that there had been unauthorized communications to their email-related equipment targeting zero-day vulnerabilities. The Meteorological Agency and Meteorological Research Institute replaced all the equipment that received unauthorized communications targeting vulnerabilities with equipment with enhanced security measures. In addition to this, some other security measures were also taken. Furthermore, from the results of the investigation, it was discovered that some of the data from emails received by meteorological offices nationwide, including the Meteorological Agency and Meteorological Research Institute, during the period from early June 2022 to late May 2023 may have been leaked outside [12].

4.3. Discussion on whether sharing of incident information is required

4.3.1. Information sharing and security/safety

In both cases, it was announced that the security incidents were caused by vulnerabilities in certain email-related equipment [11] [12]. However, the NISC and the Meteorological Agency and Meteorological Research Institute did not disclose the detailed information on the security incidents, including the model name of the equipment hit by cyberattacks and the vulnerabilities exploited. The NISC explains that the reason for not disclosing the detailed information was for security/safety purposes [13].

The Guidance for Sharing and Publication of Information on Damage from Cyberattacks [14] describes how to handle the information on zero-day vulnerabilities and how should the vulnerability information be handled when there is a concern that its disclosure may cause secondary damage. The Guidance describes that it is basically desirable to promptly share the threat information, including information on vulnerabilities, etc. Except, however, that it is desirable not to broadly share the information on possible misconfigurations in software products in general, etc., as it may attract copycat crimes, etc.

In both of these cases, it was explained that "there had been unauthorized communications targeting the vulnerabilities in the system not previously identified by the manufacturer" [11] [12]. From this statement, both cases can be considered not "cyberattacks targeting possible misconfigurations in software products in general", but "cyberattacks targeting certain products via zero-day vulnerabilities". Therefore, the non-disclosure policy taken by the three organizations is against the Guidance for Sharing and Publication of Information

on Damage from Cyberattacks [14] and is considered inappropriate.

4.3.2. Why information sharing is necessary

Some readers may wonder why it is necessary to share information on security incidents in the first place. Attackers have been developing more complex and sophisticated cyberattack methods to bypass security measures. It is difficult for an organization on its own to promptly identify and understand such attackers and cyberattacks and quickly counter them. With multiple organizations sharing the information on attackers, cyberattacks, and incidents, it is possible to obtain information on attackers and cyberattacks that could not be found by the organization on its own. This information can help identify the cause and extent of damage, preventing damage from spreading, and taking appropriate recurrence prevention measures in the event of a similar cyberattack.

The examples of the method and activities of effectively responding to incidents by sharing incident information are presented below.

The first example is the method aimed at maximizing the benefits of all the security incident affected organizations. As cyberattack methods are becoming more sophisticated these days, it is becoming increasingly difficult especially for organizations that do not have specialized security departments within the organization to establish a clear picture of the security incident on their own. If a clear picture of the security incident cannot be established, appropriate incident response, including estimation of the extent of damage, post-incident response, and recurrence prevention measures, etc., cannot be performed. In such cases, disclosing detailed security incident information held respectively by multiple organizations that had suffered similar incidents can help all the victim organizations establish a clear picture of the security incident using such information. As a result, all the victim organizations will be able to perform appropriate incident response.

The second example is the activities of the Information Sharing and Analysis Center (hereinafter “ISAC”) in which organizations within the industry participate to share information and collaborate on security incidents. ISAC is a non-profit organization originally established under a presidential decree in the U.S. In ISAC, organizations get together by industry to share, analyze, and utilize security-related information. In Japan, Financial ISAC, Transportation ISAC, and Electricity ISAC already exist. Organizations within ISAC share information on incidents that occurred in member organizations to develop security measures to prevent similar incidents from occurring in the own organization and use the information to help respond in the event of an incident.

4.3.3. Why there are organizations that do not share information

JPCERT/CC made the following comment regarding non-disclosure of incident information by the three organizations.

“(Omitted) Some have pointed out that no mention is made of vulnerabilities that have been exploited, etc. JPCERT/CC believes that, regardless of the industry the victim organizations belong to, taking the responses described in the ‘Guidance for Sharing and Publication of Information on Damage from Cyberattacks’, including disclosing the damage as well as sharing information and collaborating with specialized agencies, will not only ensure that the incident response of the victim organization is properly evaluated, but also resolve the asymmetry of information necessary for all relevant parties, including other victim organizations, to enable the country as a whole to address the attack activity.” [15]

Contrary to the benefits of information sharing activities, however, the reality is that there are organizations that do not disclose information. At present, in many cases, organizations suffering cyberattacks tend to be cautious about information disclosure, thinking that disclosure of detailed information about the security incident would negatively affect their reputation. In addition, it is considered difficult to determine, of the information on damage caused by security incidents, which information should be shared, at what timing, and to

what extent. This is also believed to be a reason that smooth and effective information sharing is not advancing.

4.3.4. Actual examples of sharing of security incident information

The timing and extent of disclosing security incident information mentioned in 4.3.3 are described in detail in the “Guidance for Sharing and Publication of Information on Damage from Cyberattacks” [14] referred to in the JPCERT/CC comment. For instance, the following two information sharing policies are presented.

1. After discovering the incident, technical information, in particular indicator information (IP address of the unauthorized communication, hash value of malware, etc.), shall be shared as soon as possible only with relevant agencies in a private setting
2. After a certain amount of investigation has been done following the discovery of the incident (typically, after the completion of the investigation), the fact that an incident has occurred, details of damage, post-incident response, etc., shall be presented in a public setting

The policy of sharing information “only with relevant agencies in a private setting” in 1. above is consistent with the abovementioned method of activities of ISAC. This allows disclosure of the information on the organization to relevant agencies in a private setting without worrying about reputation through mass media and SNSs, etc.

Not limited to ISAC, there are other cases of sharing security incident information in a private setting. For instance, security incident response practitioners from various industries also get together in the Working Group for Incident Case Analysis of the Nippon CSIRT Association to regularly share successful and failed cases of security incident response. The Chatham House rule used by this WG is also a mechanism for sharing information while preventing reputational damage. The Chatham House rule allows every participant of the meeting to take the information provided at the meeting back to his/her organization and use it freely. However, information that identifies the organization or person who is the source of the information cannot be taken. Other than these, at the grassroots level, various organizations get together in a private setting to share incident information.

At NTT DATA, when a vulnerability was discovered in the Android app “MyPallete” that we publish, vulnerability handling, including early notification and disclosure of vulnerability information, was performed as described below to contribute to the prevention of damage from security incidents. First, as described in 1. above, we immediately shared the vulnerability information and the source code that fixes the vulnerability only with the vulnerability report contact point of the IPA and relevant companies developing apps using MyPallete. After the completion of fixes to apps of relevant companies, as described in 2. above, we made an announcement about the vulnerability in collaboration with JPCERT/CC and called for updating the version that fixed the vulnerability.

4.4. Conclusion

When each organization is able to proactively and continuously share information on security incidents, society as a whole will be able to respond appropriately to security incidents. Organizations should utilize the “Guidance for Sharing and Publication of Information on Damage from Cyberattacks” and appropriately share information to maximize the benefits for both their organization and the whole of society.

5. Vulnerabilities “Ongoing serious vulnerability exploitation in Citrix products”

Omihiro Tajima
NTTDATA-CERT, Information Security Office, NTT DATA Group

There are many cyberattack methods, and the trend has changed over time. During the explosive spread of the Internet in the 1980s, there was no firewall and attackers could easily hack into the network within the organization from the Internet. Firewalls came into existence in the 1990s, making it difficult to hack into the network within the organization from the Internet. As a result, cyberattacks targeting user’s operation errors such as targeted attacks spread. Around 2010, cyberattacks targeting zero-day vulnerabilities have increased and are now mainstream.

“CVE-2023-3519”, a vulnerability in Citrix products that has caused a stir in recent years and is still ongoing, has been subject to cyberattacks targeting zero-day vulnerabilities. In October 2023, cyberattack campaigns that exploit this vulnerability to remotely execute arbitrary code to obtain user credentials took place around the world. The NTT DATA Group also suffered cyberattacks targeting this vulnerability, but no damage was caused due to proper incident response. However, NTTDATA-CERT had great difficulty responding to this vulnerability. This report provides an overview of “CVE-2023-3519”, a vulnerability in Citrix products, cyberattack methods targeting this vulnerability and countermeasures, and actual incident response and vulnerability response cases and the lessons learned in these cases in an organized manner.

5.1. Vulnerability CVE-2023-3519

NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) are appliance products used in network construction, and improve performance, strength, and security of online applications. These products are widely used around the world, and this vulnerability affected many companies. The overview of the vulnerability “CVE-2023-3519” in Citrix products, attack methods, and countermeasures are explained here.

5.1.1. Overview

The vulnerability “CVE-2023-3519” in Citrix products was disclosed on July 18, 2023. This vulnerability can be used to remotely execute arbitrary code on NetScaler ADC and NetScaler Gateway of the versions shown in Table 5-1, and has a CVSS severity score of 9.8.

Table 5-1: List of Citrix products affected by CVE-2023-3519 [16]

No.	Product name	Affected version(s)
1	NetScaler ADC and NetScaler Gateway 13.1	Versions earlier than 13.1-49.13
2	NetScaler ADC and NetScaler Gateway 13.0	Versions earlier than 13.0-91.13
3	NetScaler ADC and NetScaler Gateway 12.1	EOL
4	NetScaler ADC 13.1-FIPS	Versions earlier than 13.1-37.159
5	NetScaler ADC 12.1-FIPS	Versions earlier than 12.1-55.297
6	NetScaler ADC 12.1-NDcPP	Versions earlier than 12.1-55.297

If this vulnerability is exploited, arbitrary code may be executed remotely by a third party without authentication. In fact, cyberattacks exploiting this vulnerability have been confirmed at a certain number of companies, and there is a risk that the damage could spread. Therefore, Citrix disclosed the vulnerability information and patches.

5.1.2. Attack methods

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that attackers actually exploited this zero-day vulnerability and attacked NetScaler appliances of critical infrastructure organizations to successfully gain unauthorized access [17]. The attack flow disclosed by the CISA was as follows [18].

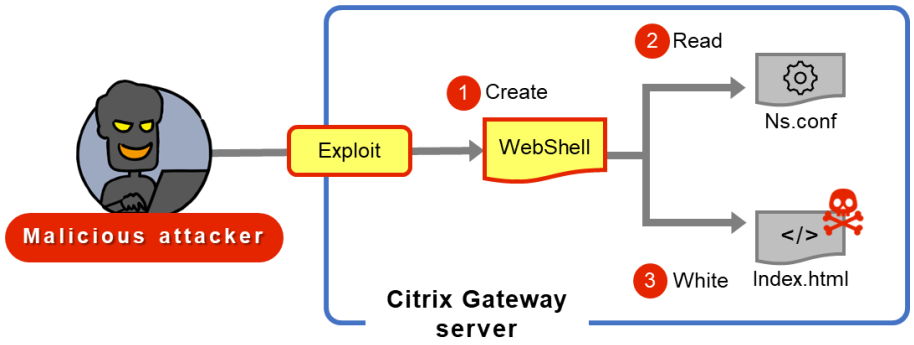


Figure 5-1: Attack flow (1) to (3) (preparation phase)

The attacker exploits CVE-2023-3519 and drops a PHP Web shell on a Citrix device under attack (1). More specifically, the attacker exploits a memory corruption vulnerability in the Citrix device to write a simple PHP Web shell on that device. The attacker uses interactive access via the PHP Web shell to obtain the content of the ns.conf file on the device (2). The attacker finds encrypted passwords in the configuration files located in /flash/nsconfig/keys/updated/* and /nsconfig/ns.conf. These passwords can be decrypted with the encryption keys stored on the NetScaler ADC. These keys are used to decrypt Active Directory credentials from the configuration files.

The attacker then collects data, including username and password entered into the form during user authentication, and prepares a JavaScript to be sent to the attack target. The attacker uses the PHP Web shell to save the JavaScript on the Citrix device and adds a code that refers to this JavaScript to “index.html” (3).

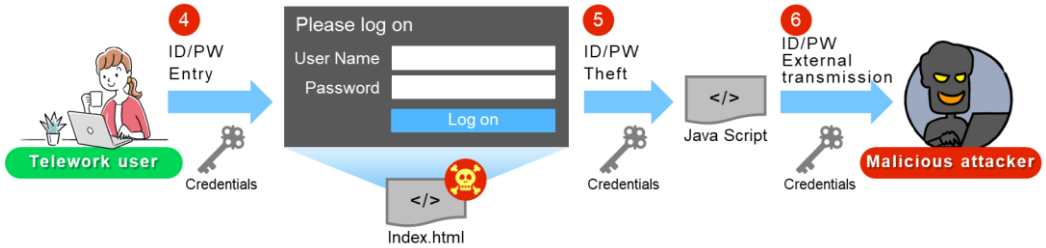


Figure 5-2: Attack flow (4) to (6) (information theft phase)

When a user enters a username and password when logging in (4), the JavaScript starts, and steals that information (5) and sends it to the attacker (6).

5.1.3. Countermeasures

A countermeasure for this vulnerability is to install the updated versions of NetScaler ADC and NetScaler Gateway with the vulnerability fixed. In addition, permanent countermeasures recommended by CISA are to implement multi-factor authentication in internal systems including NetScaler and establish robust network segmentation to prevent the lateral spread of attackers who have hacked into NetScaler appliances and other devices connected to the Internet [17].

5.2. Response and lessons learned by NTT DATA

The response to the Citrix vulnerability “CVE-2023-3519” at NTT DATA is presented here.

5.2.1. Overview of vulnerability response

(1) NTTDATA-CERT’s vulnerability response policy

The NTTDATA-CERT regularly collects vulnerability information, determines the severity, and responds accordingly. As shown in Table 5-2, for vulnerabilities of particularly high severity, the NTTDATA-CERT provides organizations and projects with the information on vulnerabilities related to the systems they own and provides instructions for response. The content of the response, including the extent of dissemination, corrective actions, and reporting deadline, varies according to the severity.

Table 5-2 NTTDATA-CERT’s vulnerability response policy by severity

Severity	Response policy
0	No response (to be responded to by each project at its own discretion)
0+	• Post alerts the internal security blog • Disseminate alerts on the corporate portal
1	• Response for the severity 0+ above • Identify organizations and systems affected by the vulnerability using the inventory information DB • Request for vulnerability response by sending alert documents to the relevant organizations
2	• Response for the severity 0+ above • Request all internal organizations to investigate and answer whether they are affected by the vulnerability • Instruct the relevant organizations to correct the vulnerability • Manage the investigation results and response status of all organizations by the ticket management system

The severity of the vulnerability CVE-2023-3519 was 1. Therefore, in accordance with Table 5-2, the NTTDATA-CERT implemented the following vulnerability response procedures.

(a) Determine the severity of the vulnerability to be 1
(b) Identify systems affected by the vulnerability
(c) Implemented the following response for organizations and projects that own the systems concerned
  1) Provide the vulnerability information
  2) Request them to investigate and answer whether the systems concerned are affected by the vulnerability
  3) Instruct them to apply patches and report the completion
(d) Manage the progress status of the systems concerned
  1) Urge them to investigate and report whether they are affected by the vulnerability
  2) Urge them to report the completion of patch application
(e) Respond to inquiries about the vulnerability

(2) Timeline of response to the vulnerability CVE-2023-3519

The response to the vulnerability CVE-2023-3519 implemented by the NTTDATA-CERT is explained here using the timeline. The NTTDATA-CERT obtained the information on CVE-2023-3519 immediately after the disclosure of this vulnerability on July 19, 2023 JST (1). The NTTDATA-CERT then instructed organizations and projects of three companies within the NTT DATA

Headquarters and the Group companies that own systems related to the vulnerability to implement the above vulnerability response (2). Three days later, on July 22, 2023, patches were applied to most systems and the vulnerability response was completed (3).

However, this vulnerability in Citrix devices was a special case in which the vulnerability was discovered to be a zero-day vulnerability sometime after the disclosure of the vulnerability information (4). As shown in Figure 5-3, cyberattacks exploiting this vulnerability in Citrix devices and the damage cause by them had started one month before the disclosure of the vulnerability (0). The NTTDATA-CERT learned that it was a zero-day vulnerability after most of the vulnerability response was completed.

Figure 5-3: Timeline of response to the vulnerability in Citrix devices

A zero-day vulnerability refers to a vulnerability exploited by cyberattacks that have occurred prior to the provision of a patch to fix the vulnerability. There are cases where by the time the vulnerability information is disclosed and the vulnerability is known, cyberattacks have already been succeeded and the targeted systems have been breached. In such cases, simply applying the patches to fix the vulnerability cannot eliminate attackers or malware already hacked into the targeted systems. The basic procedures for responding to a zero-day vulnerability is to conduct breach investigations and apply patches based on the assumption that systems have already been breached by cyberattacks.

In addition, the content of the above instructions for response given to organizations and projects that own the systems concerned by the NTTDATA-CERT (2) is different between zero-day vulnerabilities and other vulnerabilities. For zero-day vulnerabilities, prompt investigation of breaches is also instructed, and when a breach is discovered, incident response must be performed immediately.

For CVE-2023-3519, since there was no information about zero-day vulnerability at the time of disclosure of the vulnerability information, the instructions to investigate system breaches was delayed. As a result, there was a delay in discovering breaches and starting incident response.

5.2.2. Incident response to CVE-2023-3519

In some systems, patches were promptly applied as per the above instructions for response given by the NTTDATA-CERT (Figure 5-3 (2)), but it was later discovered that attackers had breached the systems. The incident response in this case is explained below based on the timeline.

<August 25>

Ⓐ It was discovered that the NetScaler Gateway server may have been breached.

Ⓑ The organization concerned reported the incident to the NTTDATA-CERT.

Ⓒ The organization contacted Citrix to learn how to investigate the breach, and started investigation to determine whether there is a breach.

(a) Detected files showing traces of a breach using a breach investigation tool.
(b) The security engineers within the organization investigated the NetScaler Gateway and found a PHP Web shell file “xxxxx.php” installed by the attacker (see Figure 5-1)
(c) Requested Citrix to analyze the detected files, and received a response that those files showed evidence of a breach due to attacks

Ⓓ Through coordination with system managers and the administrator, the NetScaler Gateway server was disconnected from the network.

Ⓔ Obtained logs of servers in the DMZ to which the attacker may have laterally spread, and conducted a breach investigation. In addition, investigation of traces of impersonation/data theft/leakage was conducted based on the following damage scenarios.
(a) Case in which the Citrix Gateway server is used as a stepping stone to further hack into adjacent servers and/or internal segments A and B
(b) Case in which remote access is used to further hack into the internal segments as an authorized VPN user

<August 26>

Ⓕ Performed restoration and version upgrade of the NetScaler Gateway server

Ⓖ The system was restored and operations were resumed

In the investigation in Ⓔ above, it was confirmed that adjacent servers in the DMZ that are in the same segment as the NetScaler Gateway server were not breached by the attacker as they had enhanced security measures in place, including login authentication and access restrictions.

It was also found that the attacker used the NetScaler Gateway server as a stepping stone to attempt hacking into the internal segments. However, as shown in Figure 5-4, the system concerned had a firewall established between the DMZ segment and internal segments to restrict access, and therefore, the attacker was unable to communicate to the internal segments and failed to attack servers and PCs in the internal segments.

In this incident, the NetScaler Gateway server was breached by exploiting a vulnerability in Citrix products. With the DMZ segmentation and enhanced security measures implemented on adjacent servers, however, the attacker was unable to further breach other servers and segment from the NetScaler Gateway server, and fortunately enough, the damage was limited to a breach of one NetScaler Gateway server.

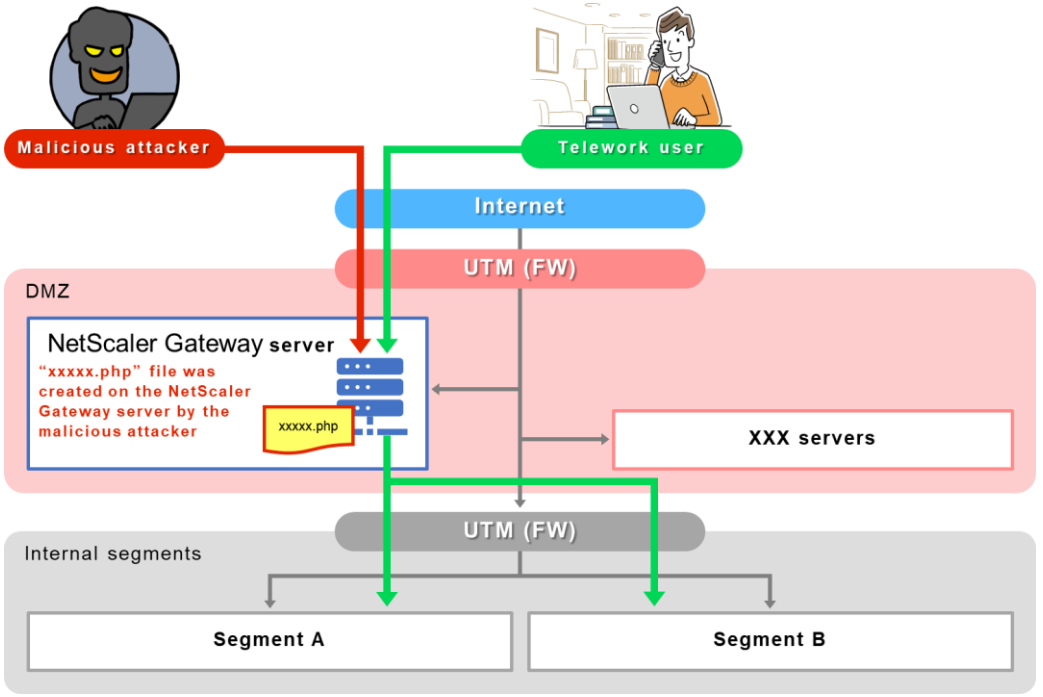


Figure 5-4: Structure of a system in which the incident occurred

5.2.3. What is important in vulnerability response

The cases of the said incident and the knowledge gained from the vulnerability response are provided here in an organized manner.

As shown in Figure 5-3, this vulnerability was disclosed to be a zero-day vulnerability three days after the disclosure of the initial information on the vulnerability. If the vulnerability response has already been completed, many organizations will hesitate to start over the vulnerability response. Even after the completion of the vulnerability response, however, a breach investigation must be conducted as promptly as possible when the vulnerability concerned is found to be a zero-day vulnerability.

In addition, for all vulnerability responses in general, a vulnerability response is often postponed due to insufficient project personnel and resulting busyness. It is important for information security operation organizations such as CSIRT and organizations/projects that own information systems to establish a system in anticipation of the occurrence of a vulnerability response and prepare for the vulnerability response flow. To be able to flexibly respond to vulnerabilities in every situation, establishment of an adequate system is essential.

Another major issue is that, after establishing information systems, there are many products that have not been updated. A need for urgent vulnerability response may arise for products to which patches are not applied and which have not been upgraded to latest versions, and attempting to apply patches to them can cause various problems. For instance, there are no procedures to apply patches, and system administrators are not sure how to obtain or apply patches. In some cases, it is required to apply all previous patches or upgrades before applying patches to fix the vulnerability. A need for vulnerability response arises for any products. Therefore, regular updates during normal times are important. The desirable frequency is at least once every year to once every quarter.

5.3. Conclusion

There are various cyberattack methods. Of which, those that cause the most significant damage are cyberattacks targeting zero-day vulnerabilities. According to the National Cyber Security Centre (NCSC), with a background that system breaches using phishing attacks are becoming difficult with the advancement of security measures in recent years and that finding zero-day vulnerabilities is not so difficult, attackers seem to be starting to change their tactics to use the methods of breaching systems by attacking zero-day vulnerabilities in network products [19]. In recent years, attackers are constantly searching for zero-day vulnerabilities in all the network devices connected to the Internet and seeking attack opportunities.

This chapter presented the vulnerability response to “CVE-2023-3519”, a zero-day vulnerability in Citrix products, and the incident response involving it. Many of the readers of this report may consider that zero-day vulnerabilities only occur in irregular cases. The author of this chapter was one of them, too. Looking back at FY2023 once again, however, we can see that the number of zero-day vulnerabilities disclosed and the amount of damage caused were very high and are increasing. To protect our organizations from cyberattacks, we must change our thinking and understand that zero-day vulnerabilities are not limited to irregular cases. To protect our company, it is important to correctly understand zero-day vulnerabilities and not to miss the necessary responses.

6. Malware/ransomware “Future ransomware attack methods, considering the emergence of no-ware ransom”

Naoki Shimatani, Cyber Security Department, NTT DATA Group

Ransomware attacks remain a threat across the world. However, the idea that “ransomware = encryption” may need to be revised. This is because ransomware that does not encrypt files, called “no-ware ransom”, has appeared. This section discusses what no-ware ransom is and how did it emerge, and explains security measures against attacks using no-ware ransom and future ransomware attack methods.

6.1. What is no-ware ransom?

The term “no-ware ransom” has been mentioned in “Threat Situation in Cyberspace, etc., in the First Half of 2023” published by the National Police Agency in September 2023 [20], and it is called “encryption-less ransomware” overseas.

The difference between no-ware ransom and ransomware is whether to encrypt files. Ransomware encrypts files on infected computers. The attacker who launched the ransomware attack demands a ransom in exchange for the decryption of the encrypted files. In addition, ransomware steals files from the infected computers. The attacker sometimes demands a ransom for not disclosing those stolen files to the public. In contrast, no-ware ransom attacks do not encrypt files, and a ransom is demanded for not disclosing the stolen files to the public. In other words, it is a ransomware without the action to encrypt files, and is an attack technique that uses file disclosures as a threat to demand a ransom. It is not an entirely new attack that has emerged, but is a variant of a ransomware attack.

6.2. History of ransomware attacks

The difference between the existing ransomware and no-ware ransom can be readily understood. To understand the reason for the emergence of no-ware ransom, it is necessary to understand the history of crimes using ransomware. This subsection briefly looks back on the history of ransomware changes.

6.2.1. Early years

Malware that encrypts files and demands a ransom existed more than 30 years ago. The famous one is “AIDS Trojan”. It is also called “PC Cyborg Trojan”. It emerged in 1989, encrypting the names of files on the infected computers and demanding a ransom for decrypting them. It is quite different from the current ransomware, including non-encryption of file data and infection through floppy disks, but the concept of encrypting important files and demanding a ransom is the origin of the current ransomware attacks.

But then why did it not become as prevalent as it is today. There could be a variety of factors, but the fact that the attacker could not easily prepare a method to conceal its identity and obtain the ransom could have been critical. In the

case of a bank transfer, the police can identify the sender and recipient. Therefore, it was difficult for cybercriminals to conceal their identities.

6.2.2. Growing years

The situation changed in the 2010s with the emergence of cryptocurrencies such as Bitcoin. In the case of cryptocurrencies, the address used for transactions is not linked to personal information such as the name of the person. For this reason, it is possible to track the transaction history of a specific address, but the owner of the address cannot be identified because the cryptocurrency system does not have personal information of the address owner. The emergence of cryptocurrencies provided criminals with a method to obtain the ransom without having their identities identified.

A ransomware that is famous for demanding a ransom in cryptocurrencies is “CryptoLocker,” which emerged in 2013. Since the time when CryptoLocker went on a rampage, various ransomware has emerged.

In addition, RaaS (Ransomware as a Service), which provides ransomware attacks as a Web service, also emerged. It is a service that provides ransomware, infrastructure, and tools necessary for conducting ransomware attacks for a fee. This enables attackers to conduct ransomware attacks to the target without having technological skills and funds to develop, maintain, and operate ransomware and infrastructure used for attacks. In addition, ransomware developers can earn money from other attackers as a fee for using RaaS without conducting ransomware attacks themselves. As was just described, an ecosystem for ransomware attacks has been established and as a result, ransomware attacks became more active.

6.2.3. Diversified attack methods

While ransomware was on the rampage, companies at risk of being attacked have also advanced their security measures. A representative security measure is data backup. Even if data on the computer is encrypted by ransomware, the data can be restored if a backup of the data is obtained in advance.

Cybercriminals too have changed their attack methods. The ransomware called “MAZE” started using double extortion schemes in which a ransom is demanded by, in addition to encrypting files, threatening to disclose the stolen information. Even if data has been backed up, they can still demand a ransom by threatening to disclose the data.

As described above, ransomware developers have used various mechanisms to change ransomware functions and attack methods.

6.3. Discussion on the reasons for the emergence of no-ware ransom

Based on the history of ransomware changes, the reasons why no-ware ransom emerged are discussed here. Discussions are mainly based on the viewpoints of ransomware developers.

6.3.1. Measures against data encryption attacks

As of 2023, the rate of ransom payment for ransomware attacks is declining worldwide [21].

The first reason is that even if data is encrypted as a result of ransomware attacks, the data can be restored if the data is backed up. Therefore, many companies now back up their data [20].

The second reason is that public agencies and security vendors publish tools that can decrypt files encrypted by ransomware on their websites, such as the website “No More Ransom” [22]. In many cases, public agencies such as FBI investigates ransomware infrastructure to obtain and publish the decryption keys [23]. By using these decryption tools and decryption keys, data can be restored without paying a ransom to the attacker to receive the decryption key.

As just described, cases in which the victim organizations do not pay a ransom are assumed to be increasing because even if they are victimized by ransomware attacks and have their data encrypted, the data can be restored. In

the case of no-ware ransom, however, attackers can demand a ransom by threatening the victims regardless of whether the data can be restored. Attackers must have determined that demanding money using no-ware ransom that only steals data is a more efficient mechanism to obtain money.

6.3.2. Easy to develop, maintain, and operate, and quick to gain profit

Since no-ware ransom does not encrypt files, there is no need to implement the encryption function implemented in ransomware. The encryption functions is a major function of ransomware. No need to develop the encryption function of ransomware means that person-hours required for developing infrastructure related to the encryption function and the development costs, including development personnel, can both be reduced. In addition, the development period from the start of the ransomware development to the receipt of the ransom or the fee for using RaaS after the attacks are started can also be reduced accordingly. If the development period can be reduced, it is possible to launch ransomware attacks by exploiting a new vulnerability before the target companies take security measures for that vulnerability. In addition, since there is also no need to manage keys used for encryption and decryption, infrastructure operation can be easier.

6.3.3. Fatigue in technical support for decryption

If the victim organization fails to restore data after paying the ransom, the reputation of the ransomware attack/attacking group will be damaged, and other victims will become hesitant to pay the ransom to that ransomware attack/attacking group. Therefore, the attacking group sometimes had to provide support for the decryption problems of the victim organization.

In some cases, RaaS also provides technical support to the attackers after purchase. Even attackers with low technical skills can conduct ransomware attacks if they sign up for RaaS and use technical support. For attackers with low technical skills, technical support is a great advantage.

Attackers and RaaS providers must deal with the problems of being able to perform encryption or decryption properly, and there were cases where the support burden is higher than expected [24]. It is assumed that such technical support has been a significant burden on attackers and RaaS providers. With no-ware ransom, there will be no situation where encryption and decryption cannot be performed, and therefore, technical support related to encryption and decryption is not needed.

6.4. Speculation about future ransomware attacks

Based on the above, changes to future ransomware attack methods are discussed here.

First, it is assumed that no-ware ransom will become more prevalent. Since many companies now back up their data [20], it is assumed that the damage from conventional ransomware attacks that encrypt data will stabilize. However, the threat of ransomware attacks will continue to exist, and, in place of ransomware attacks that encrypt data, it is assumed that no-ware ransom will increase.

Second, it is assumed that RaaS for no-ware ransom will increase. For RaaS for no-ware ransom, there is no need to implement the encryption function and manage keys, and therefore, technical support is expected to be easier than conventional RaaS. For this reason, even organizations without advanced technologies can develop and provide RaaS. Therefore, it is assumed that the supply of RaaS will increase and so will attacks using RaaS.

6.5. Future anti-ransomware policy

Attacks using no-ware ransom use the same attack methods as ransomware

that encrypt data except for the encryption part. Therefore, organizations can prevent attacks and restore data with conventional security measures against ransomware. In cases where no-ware ransom attacks could not be prevented and resulted in infection and hacking into internal systems, measures to prevent confidential data from being taken outside the company are effective countermeasures against no-ware ransom. For instance, a mechanism to disallow transmission of files and data to the attacker's server or RaaS and encryption of confidential data are proposed countermeasures.

Organizations with the response policy to pay the ransom when attacked by ransomware, however, need to change their response in the future. According to a study by Sophos in 2023, the number of the cases in which organizations with cyber insurance that includes a rider for damage from ransomware restored their data by paying the ransom is four times larger than that of the cases in which organizations without cyber insurance restored their data [25]. This shows that many companies use cyber insurance to pay the ransom. Because of the regulations of the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury [26] and that the U.S. Government is also considering to regulate the ransom payment [27], paying the ransom will become difficult in the future. Paying the ransom by using cyber insurance will likely be impossible.

In Japan, cyber insurance does not cover ransom payments [28], and therefore, the situation is different from other countries. Since Japanese organizations do not depend on the method of paying the ransom by insurance coverage, is it assumed that if the regulations on the ransom payment are tightened, instead of paying the ransom to restore the data, they will make more investments in measures against malware/ransomware.

7. Outlook

Election and Deepfakes

2024 is the “election year” in which a series of elections take place in countries and regions that have significant impacts on global affairs. Starting with the Taiwan presidential election in January, followed by the Russian presidential election in March, the EU’s European Parliament election in June, and finally the U.S. presidential election in November. In Japan, the possibility of a snap general election in 2024 cannot be ruled out. During these election periods, there is a risk of election interference caused by the spread of deepfake content such as fake audio, images, and videos created by generative AI. In fact, in the September 2023 general election in Slovakia, fake audio data disclosing vote-buying by a candidate was posted on SNS. The audio data was deleted within a few hours after the post, but only after it had already been spread. It is believed that this post affected the outcome of the vote. In recent years, anyone can easily create deepfake content that more precisely impersonates others using generative AI. If deepfake content impersonating a candidate with negative information is massively spread on SNS, etc., during the election period, it can have a significant impact on the voting results. If a large amount of deepfake content circulates, voters will not be able to distinguish the deepfake content from the real content. Voters will have doubts about all the content of the candidate.

As described in the Outlook article of the Quarterly Report 2nd Quarter of 2021, development of AI technologies that can detect deepfakes is also advancing. In future, tools for detecting deepfakes will catch up with deepfake technology. Even if such tools become available, however, not all voters will have access to those tools. If deepfake content that interferes with the election cannot be prevented, Internet election public relations activities may decline in the future.

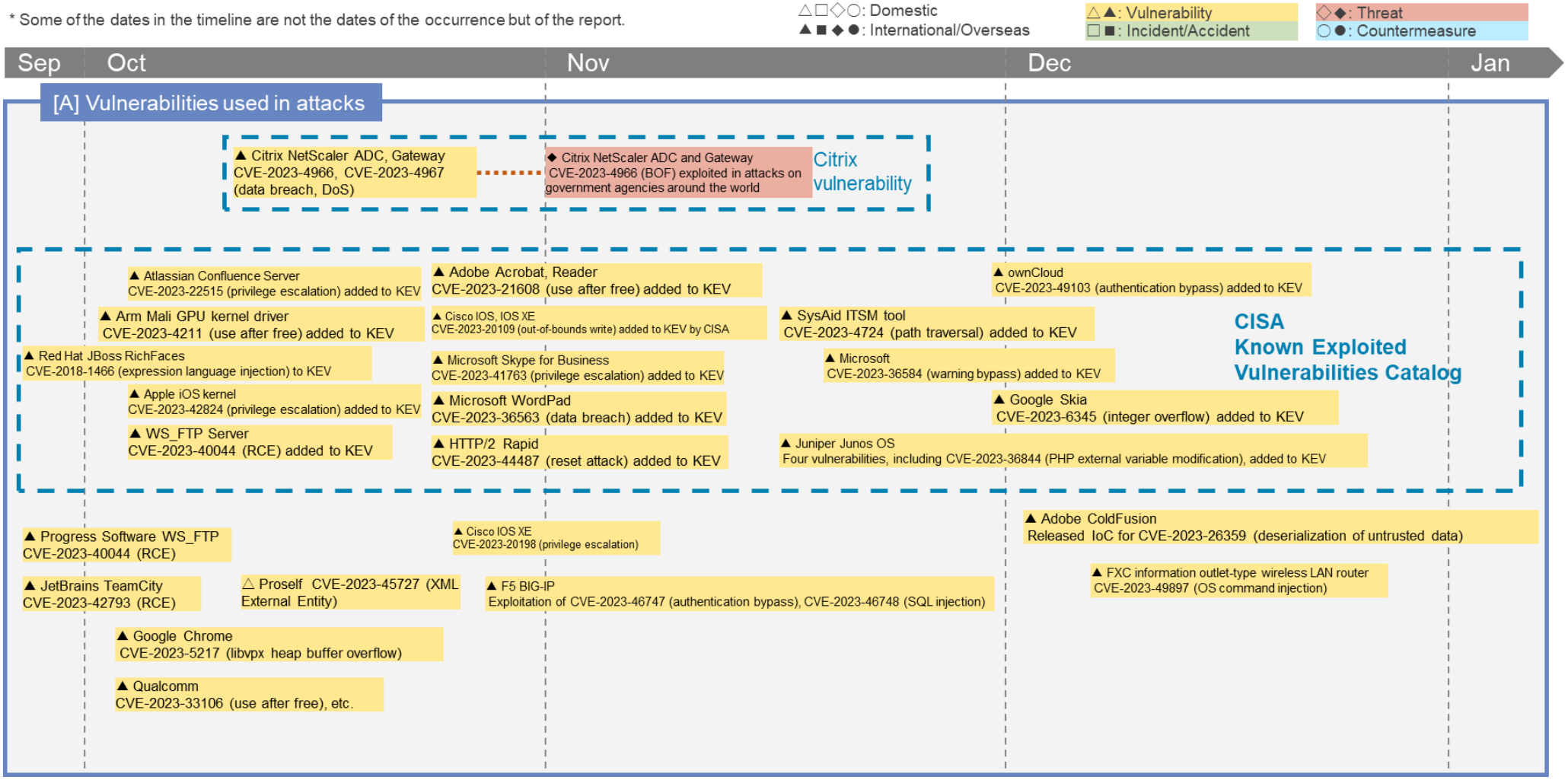
Bitcoin price rise and increase in cryptojacking

Cryptojacking is an activity of mining cryptocurrencies by using other people’s computers in an unauthorized manner. Because mining requires high-performance computer resources, criminals infect other people’s computers with mining malware and use those computer resources in an unauthorized manner for mining. The computers infected with mining malware become slower in processing speed and consume more power, etc.

On March 11, 2024, the Bitcoin price surpassed $72,500, reaching a new market high. Since the profitability of mining increases as the price of cryptocurrencies rises, cryptojacking by criminals also increases. In 2023, in response to the increase in the Bitcoin price, cryptojacking increased around the world. As the Bitcoin price is also increasing in 2024, cryptojacking and damage from it are projected to continue to increase.

8. Timeline

Yuhei Terashi / Ryotaro Tanaka, NTTDATA-CERT, Information Security Office, NTT DATA Group

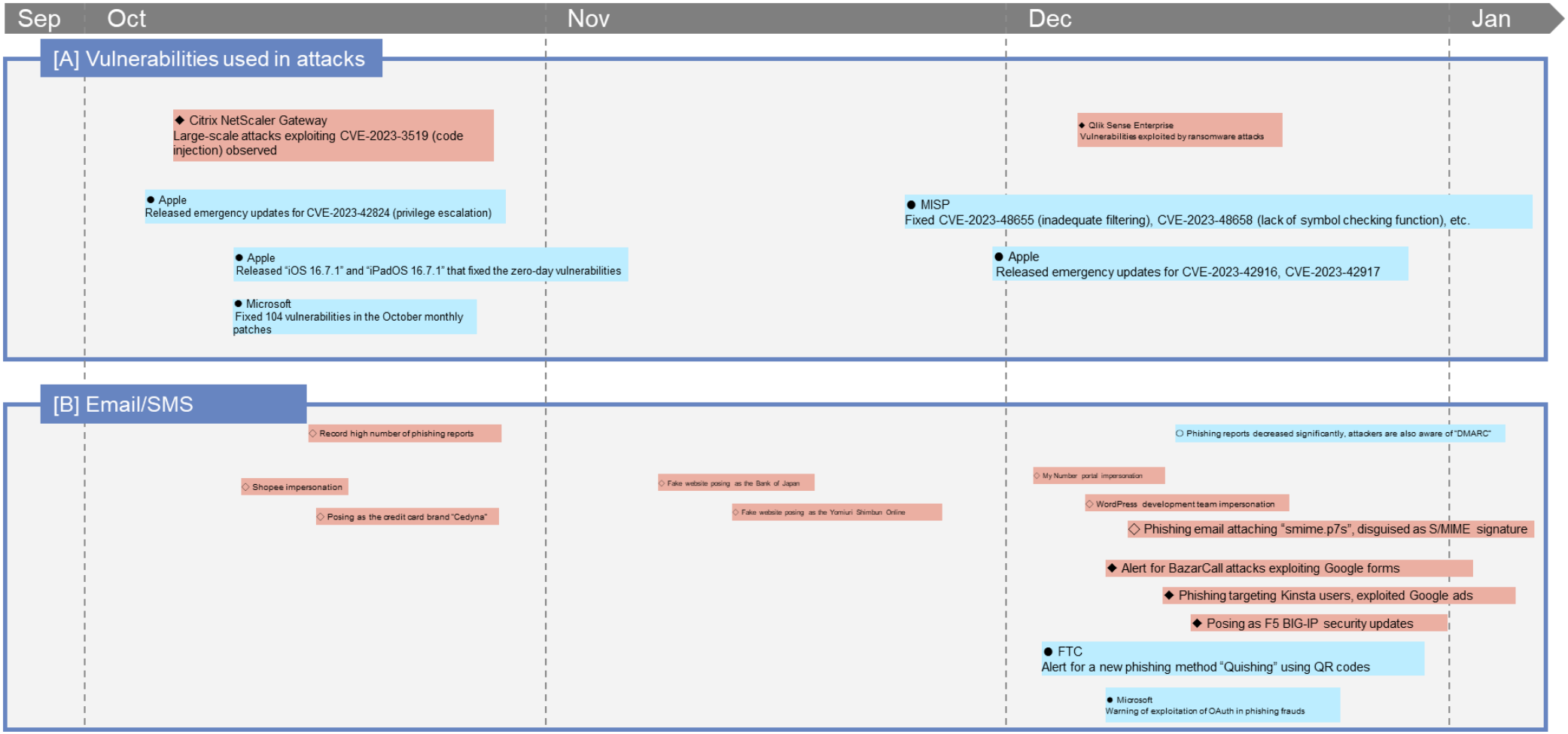


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

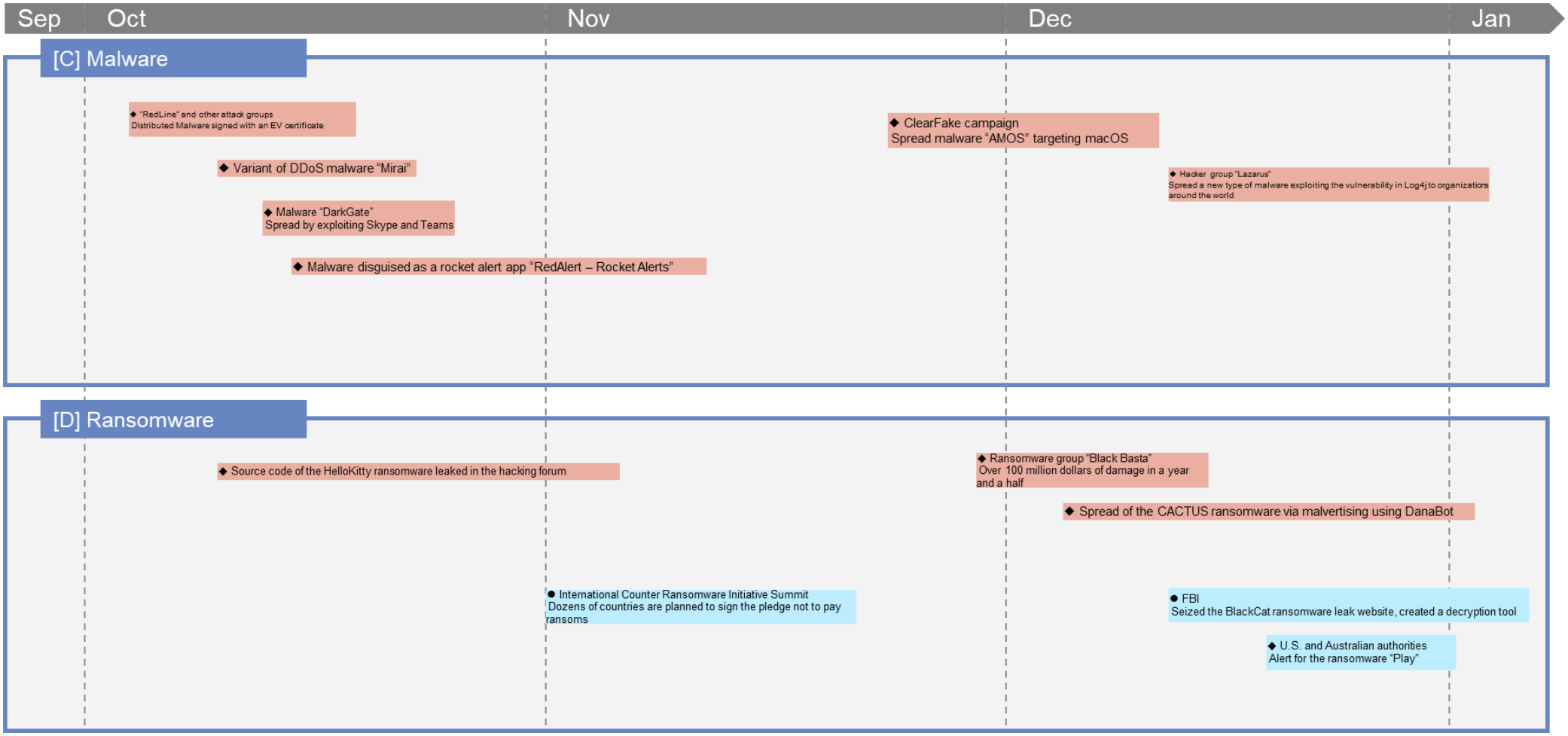


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

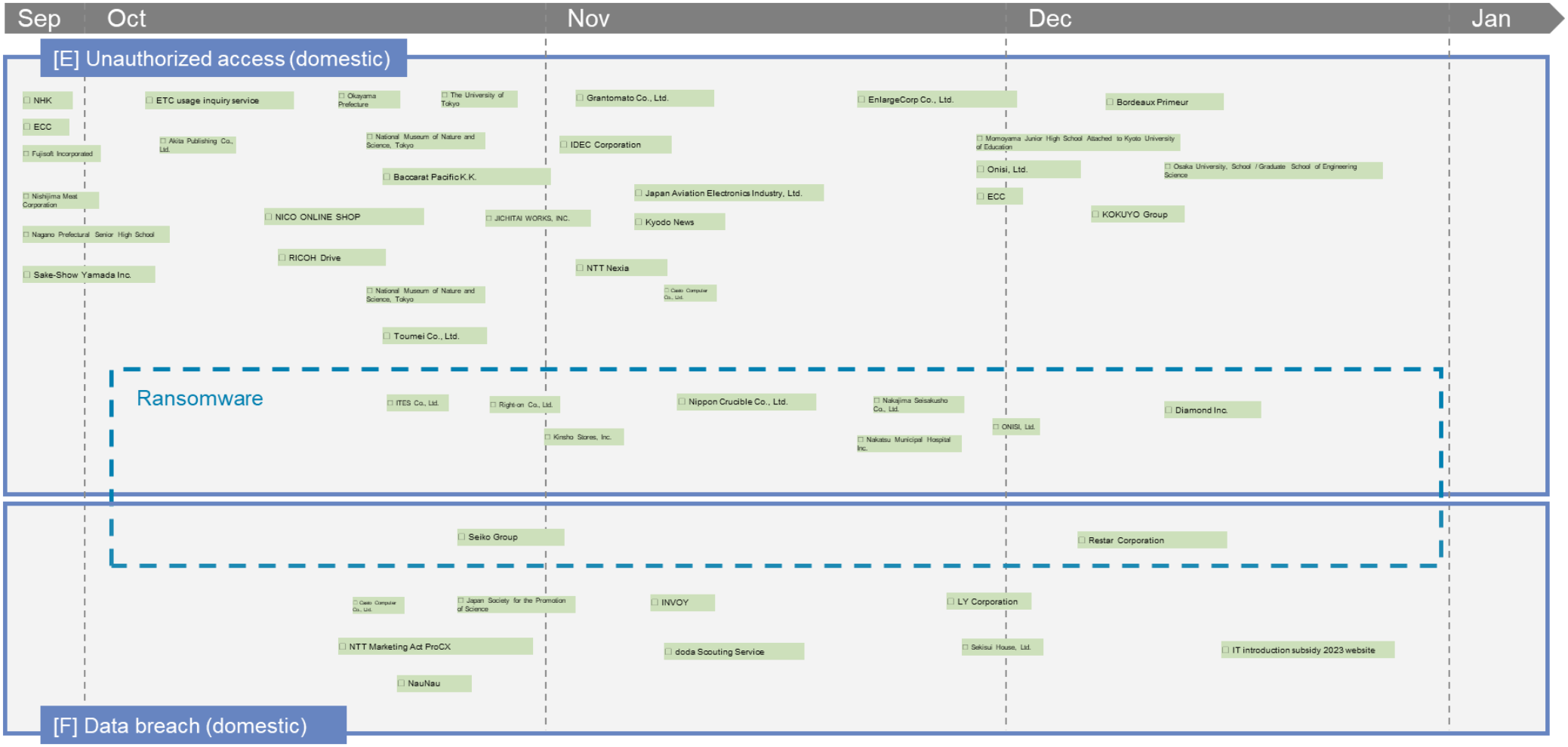


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

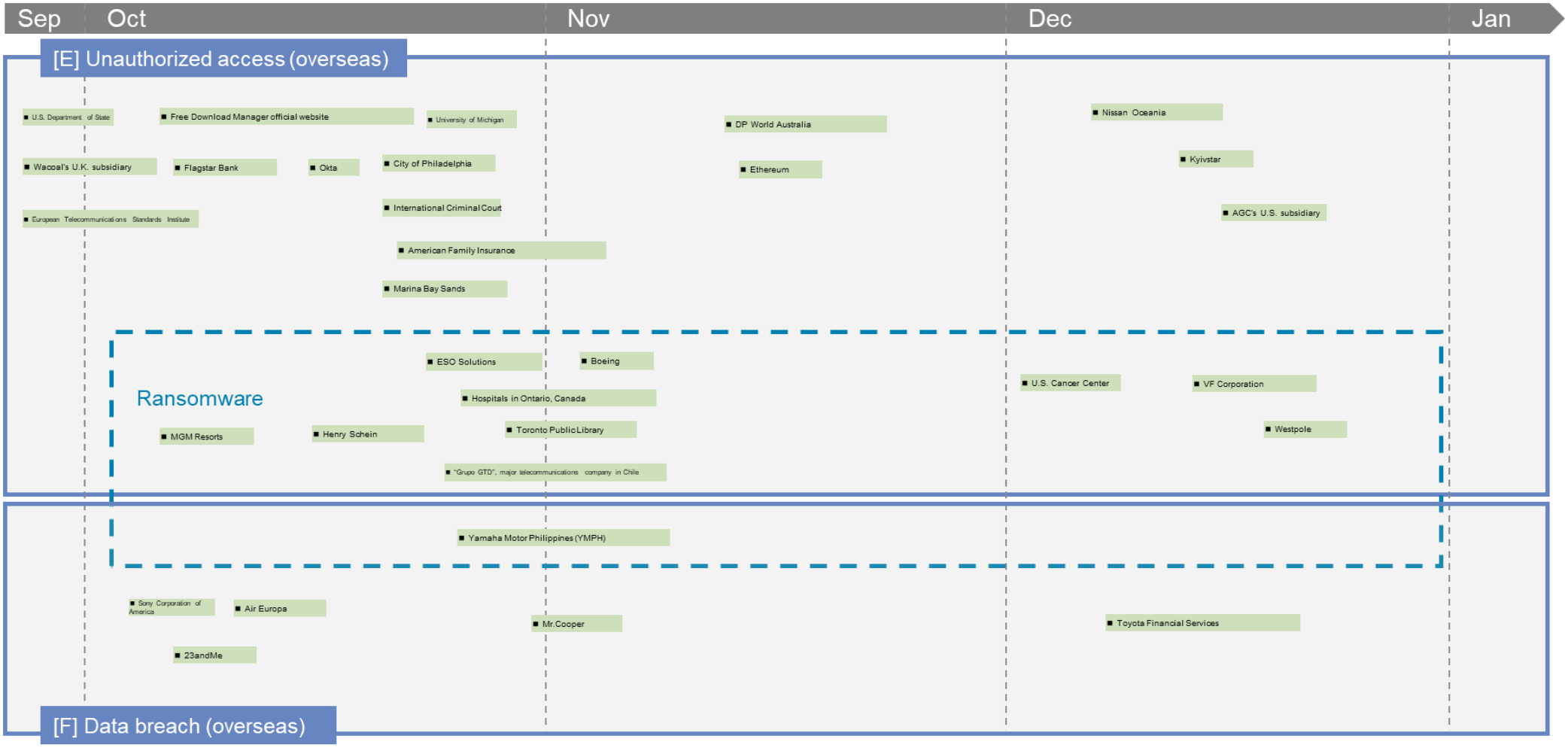


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

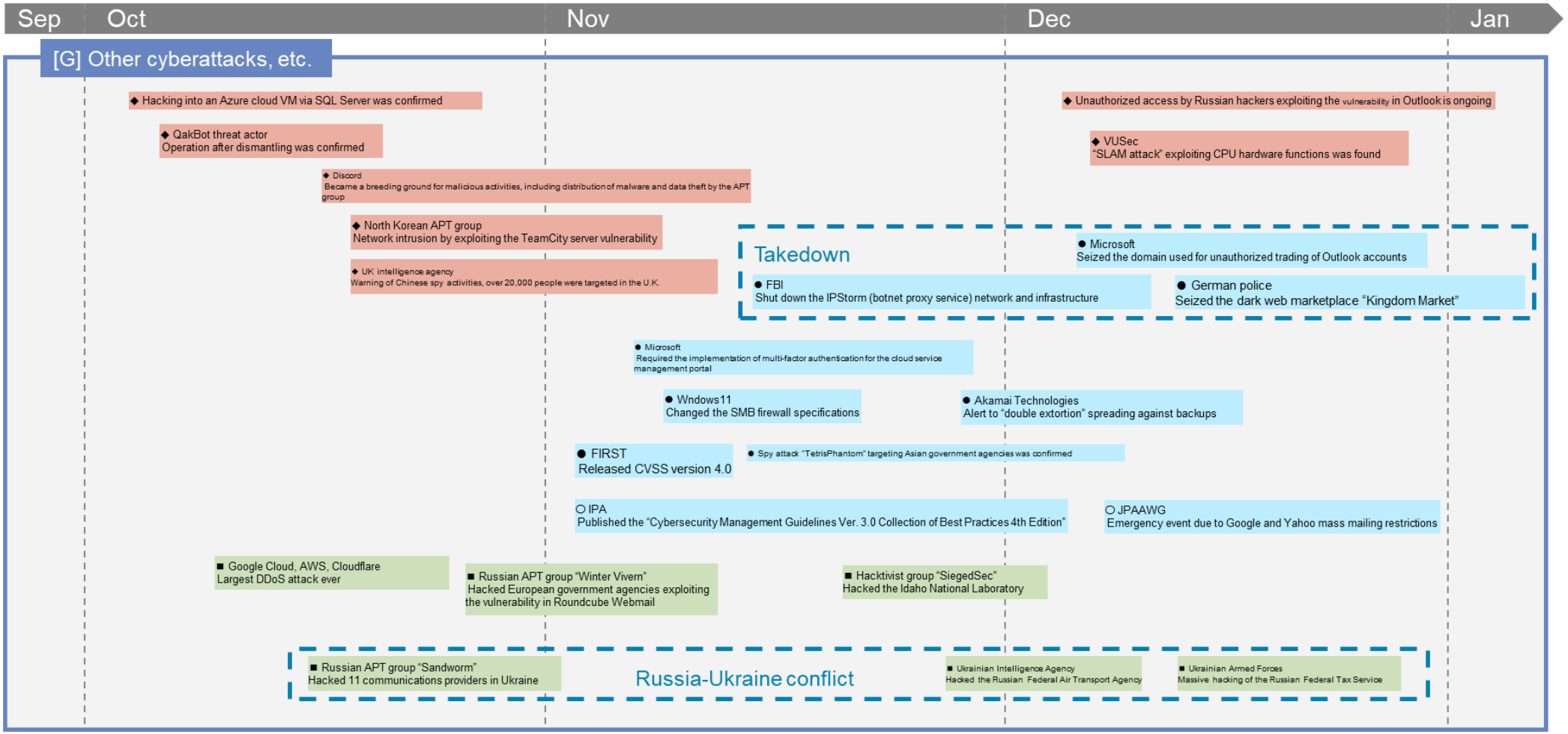


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure



References

[1] デジタル庁, “デジタル社会の実現に向けた重点計画,” 9 Jun. 2023. [オンライン]. Available: https://www.digital.go.jp/policies/priority-policy-program.

[2] デジタル庁, “次期個人番号カードタスクフォース（第1回）,” 7 Sep. 2023. [オンライン]. Available: https://www.digital.go.jp/councils/mynumber-card-renewal/8f5526a5-1a75-40e9-859b-281defa27d6c.

[3] デジタル庁, “次期個人番号カードタスクフォース（第3回）,” 26 Dec. 2023. [オンライン]. Available: https://www.digital.go.jp/councils/mynumber-card-renewal/088eeae8-1d38-4267-8ac4-d576eabf2d8d.

[4] CRYPTREC, Mar. 2022. [オンライン]. Available: https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf.

[5] NTT DATA, “グローバルセキュリティ動向四半期レポート,” 19 5 2023. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2022_3q_securityreport.pdf?rev=32ca0531eeb241a59ab983dced8f1a6e.

[6] FIDOアライアンス, “2023年にパスキーによるパスワードレスサインインが70億以上のオンラインアカウントで利用可能になり、FIDO認証の採用が急増,” 7 12 2023. [オンライン]. Available: https://fidoalliance.org/fido-authentication-adoption-soars-as-passwordless-sign-ins-with-passkeys-become-available-on-more-than-7-billion-online-accounts-in-2023/?lang=ja.

[7] COMMISSION, U.S. SECURITIES AND EXCHANGE, “Cybersecurity Disclosure,” [オンライン]. Available: https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214.

[8] European Commission, “EU Cyber Resilience Act,” [オンライン]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[9] 個人情報保護委員会, “漏えい等報告・本人への通知の義務化について,” [オンライン]. Available: https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/.

[10] 総務省, “我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言,” [オンライン]. Available: https://www.soumu.go.jp/main_content/000666221.pdf.

[11] 内閣サイバーセキュリティセンター, “内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について,” [オンライン]. Available: https://www.nisc.go.jp/news/20230804.html.

[12] 国土交通省気象庁, “気象庁及び気象研究所のメール関連機器に対する不正通信の発生について,” [オンライン]. Available: https://www.jma.go.jp/jma/press/2308/04a/press_security_20230804.html.

[13] 日経XTECH, “JPCERT／CCがNISCに苦言？ メール漏洩の情報公開巡り,” [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/15730/.

[14] 内閣サイバーセキュリティセンター, “サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会,” [オンライン]. Available: https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html.

[15] JPCERT/CC, “電子メール関連システムからのメールデータ漏えい被害が公表されている件について,” [オンライン]. Available: https://www.jpcert.or.jp/press/2023/PR20230807_notice1.html.

[16] 独立行政法人 情報処理推進機構, “Citrix ADC および Citrix Gateway の脆弱性対策について(CVE-2023-3519 等),” [オンライン]. Available: https://www.ipa.go.jp/security/security-alert/2023/alert20230719.html.

[17] CISA, “Threat Actors Exploiting Citrix CVE-2023-3519,” [オンライン]. Available: https://www.cisa.gov/sites/default/files/2023-07/aa23-201a_csa_threat_actors_exploiting_citrix-cve-2023-3519_to_implant_webshells.pdf.

[18] securityintelligence.com, “X-Force uncovers global NetScaler Gateway credential harvesting campaign,” [オンライン]. Available: https://securityintelligence.com/x-force/x-force-uncovers-global-netscaler-gateway-credential-harvesting-campaign/.

[19] National Cyber SecurityCentre, “Products on your perimeter considered harmful,” [オンライン]. Available: https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter.

[20] 警察庁, “令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について,” 21 9 2023. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf.

[21] Coveware, “New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying,” 26 1 2024. [オンライン]. Available: https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

[22] NO MORE RANSOM, “The No More Ransom Project,” [オンライン]. Available: https://www.nomoreransom.org/ja/index.html.

[23] The Register, “FBI develops decryptor for BlackCat ransomware, seizes gang's website,” 19 12 2023. [オンライン]. Available: https://www.theregister.com/2023/12/19/blackcat_domain_seizure/.

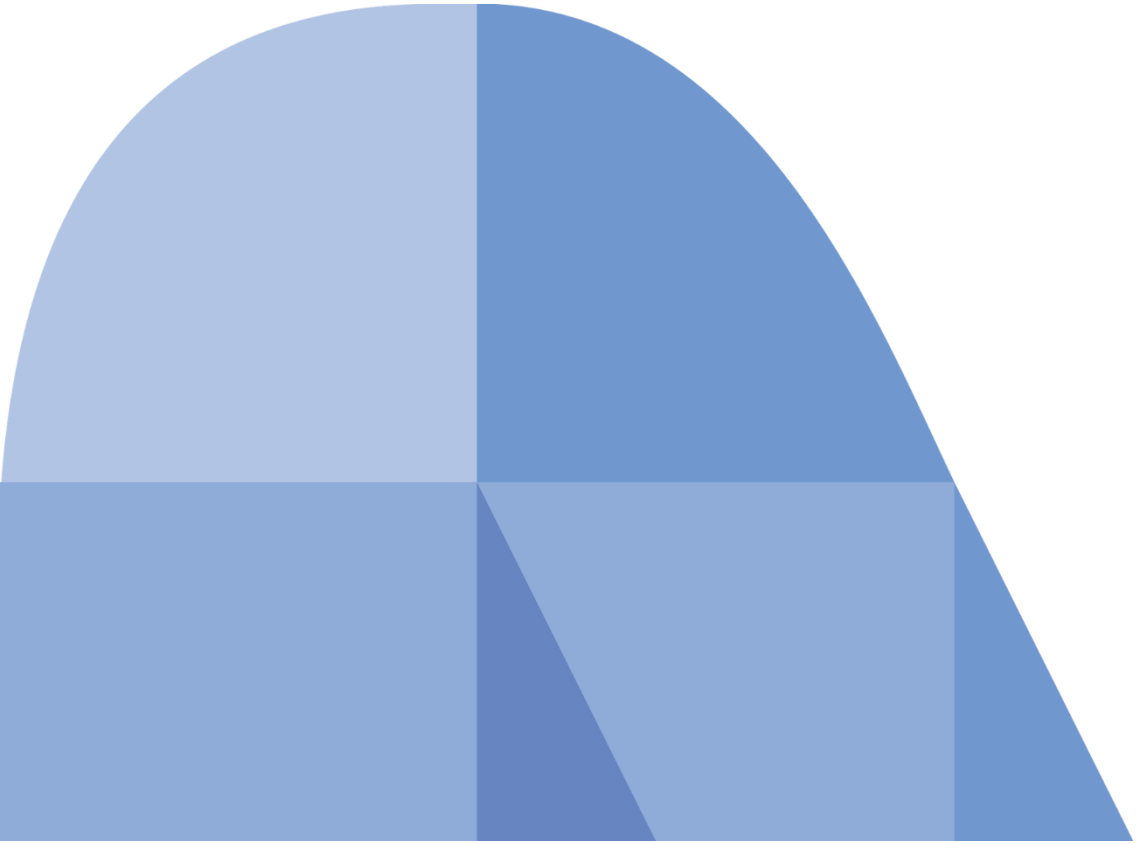
[24] The Register, “When are we gonna stop calling it ransomware? It's just data kidnapping now,” 9 10 2022. [オンライン]. Available: https://www.theregister.com/2022/10/09/extortion_ransomware_threats_category/.

[25] Sophos, “サイバー保険の導入：サイバーディフェンスの最前線で果たす重要な役割,” 3 5 2023. [オンライン]. Available: https://news.sophos.com/ja-jp/2023/05/03/cyber-insurance-adoption-the-critical-role-of-frontline-cyber-defenses-jp/.

[26] 米国OFAC, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://ofac.treasury.gov/media/48301/download?inline.

[27] Cybersecurity Dive, “White House considers ban on ransom payments, with caveats,” 8 5 2023. [オンライン]. Available: https://www.cybersecuritydive.com/news/white-house-considers-ransom-payment-ban/649673/.

[28] 一般社団法人 日本損害保険協会, “サイバー保険とは | サイバー保険 | 日本損害保険協会,” [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/about/.



Published on June 19, 2024
NTTDATA-CERT, Information Security Office, NTT DATA Group

(Writers)
Yuto Kihira
Hidehito Hodoyoshi
Reiko Tasugi
Akira Takeda
Omihiro Tajima
Naoki Shimatan
Yuhei Terashi
Ryotaro Tanaka

(Editors)
Shinichi Oshima
Hisamichi Ohtani
Koji Sugimura
Hirotaka Ogasahara
Shusuke Maeda
Kazuya Tanahashi
Daisuke Miyazaki
Takayoshi Sawada

nttdata-cert@kits.nttdata.co.jp