Quarterly Report on Global Security Trends

2nd Quarter of 2022

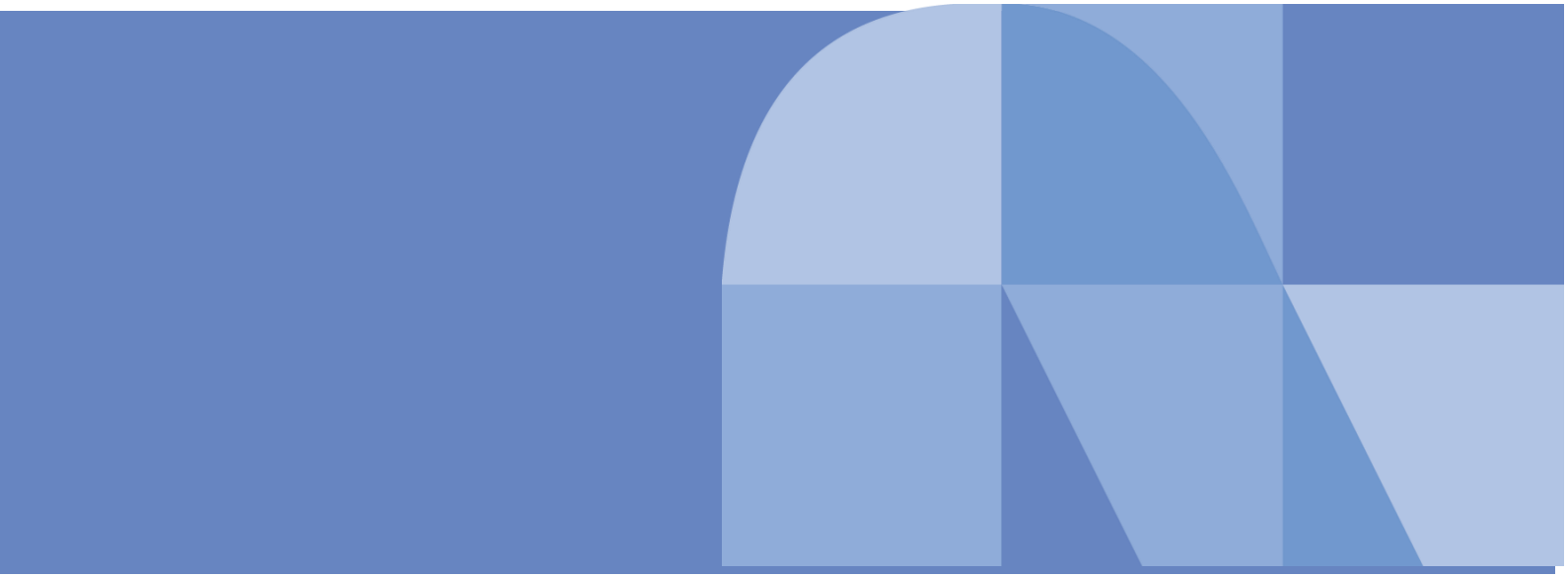


Table of Contents

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.

Featured topic, "Risks and countermeasures in telework after Covid-19"

Due to the Covid-19 pandemic, many companies have switched to telework and other remote-work centered work styles in order to allow their employees to avoid crowded places, and have suppressed employee attendance at the workplace. In doing so, in order to prioritize business continuity, many companies added special/exceptional rules to their internal security rules, which has led to an increase in the number of occasions where causes of security incidents arise.

In anticipation of the post-Covid-19 era, it will be necessary to consider abolishing the special/exceptional rules to restore the original rules. Alternatively, the rules themselves should be updated after analyzing the risks of the special/exceptional rules and adding security measures that address the security issues.

Featured topic, "Revisiting the revision of the Personal Information Protection Act"

With the revised Personal Information Protection Act that came into effect in April 2022, the attention on the responsibilities that businesses must adhere to has increased. Points to note include “mandatory reporting to the Personal Information Protection Commission and notification to the individual,” as well as “extraterritorial application of the law and cross-border data transfers.”

It is important for businesses to respond by regularly reviewing their rules and procedures in accordance with the revisions that are made to the Personal Information Protection Act every three years. In addition, as technology advances and social conditions change, businesses need to review how they handle personal information to optimize it for the times.

Vulnerability, "MFA fatigue attacks exploiting a multi-factor authentication vulnerability"

Damage has been caused by multi-factor authentication (MFA) fatigue attacks that exploit push notifications for MFA.

First, it is necessary to consider technical measures such as improving the push notification method or changing it to other methods. It is also important to raise awareness of MFA fatigue attacks, and to take organizational and human countermeasures such as never allowing login for push notifications that the user does not remember, and reporting any suspicious push notifications to the system administrator and changing passwords.

Malware and ransomware, “Advanced methods of infection and detection evasion of malware targeting Linux"

In the second quarter of FY2022, there was an increase in the number of malware attacks for monetary purposes targeting Linux-based machines among servers in the cloud and IoT devices. In addition, advanced malware targeting Linux has been found that is difficult to detect. Among such advanced malware, we present Orbit and Shikitega, both of which are difficult to detect. Orbit has a characteristic method of evading malware activity detection after infection. For example, even if the user investigates communication logs on the infected machine, they will not be able to see the communication records of Orbit's backdoor. Shikitega is characterized by its method of evading detection until infection is successful, using multiple methods. For example, it evades pattern matching-based detection through methods such as an infection chain, which installs malicious code in three stages or an encoder called "Shikata Ga Nai (No way to avoid)" to obfuscate shellcode.

2. Featured topic, "Risks and countermeasures in telework after Covid-19"

2.1. Risks and countermeasures in telework after Covid-19

2.1.1. The new normal that has become commonplace

In 2020, a new infectious disease, Covid-19, spread and companies implemented various measures to continue their businesses.

In 2020, the outbreak of Covid-19 occurred. "Telework" was introduced hastily.
In 2021, a review of the rules regarding telework was implemented.
In 2022, telework is becoming established as a way of working in the post-Covid-19 era (current).

The IPA conducted a survey in 2020 and 2021 called "Survey on the Actual Status of Telework Security in Companies and Organizations" to investigate the impact on security measures and business outsourcing contracts at various companies. A total of 508 companies, including 239 client companies and 269 contractors, responded to the questionnaire for the "2021 Survey on the Actual Status of Telework Security in Companies and Organizations.” Based on the responses to the "2021 Survey on the Actual Status of Telework Security in Companies and Organizations" questionnaire, this article will examine the special/exceptional rules that were temporarily adopted during the introduction of telework.

2.1.2. Rules treated as special/exceptional

Due to the Covid-19 pandemic, many companies have switched to a telework-centered work style in order to allow their employees to avoid crowded places, and have suppressed employee attendance at the workplace. Because of the major changes in the way they work and the priority given to business continuity, special/exceptional rules were added to the internal security rules. The following rules are some examples.

- Taking home company-provided PCs that can store confidential information
- Using personally owned PCs for work purposes (i.e., Bring your own device, “BYOD”)
- Printing confidential information outside the company (at home, satellite offices, etc.)

Since these rules were discussed in the 2021 survey results as well, it is clear that they have remained as special/exceptional rules until now in the post-Covid-19 era. In the following section, we will examine the security risks that these special/exceptional rules may cause.

2.1.3. Relationship between special/exceptional rules and incidents

What were the actual security incidents that occurred after April 2020? According to the survey results, the following three types of security incidents occurred frequently among the client companies and the contractors.

- Malware infection on PCs used for telework (common to both client companies and contractors)
- Loss or theft of PCs used for telework (client companies)
- Loss or theft of paper materials, documents, USB flash drives, and other electronic recording media (contractors)

First, malware infection on PCs used for telework is closely related to “Using personally owned PCs for work purposes (BYOD)” and is likely to occur due to insufficient security measures on personally owned PCs. Company-provided PCs are equipped with multiple layers of cutting-edge security products such as URL filters, EDR, and SWG (Secure Web Gateway), but personally owned PCs typically only have antivirus software installed. In addition, personally owned PCs are used to browse a variety of websites without restrictions, unlike those used solely for work purposes. Therefore, personally owned PCs are more likely to come into contact with suspicious/unidentified websites, software, emails, etc., which are the main causes of incidents, and coupled with inadequate countermeasures, they are prone to incidents.

Loss or theft of PCs used for telework is related to "Taking home company-provided PCs that can store confidential information." Loss and theft are caused by the same things as before the outbreak of Covid-19, e.g., when people do not always carry their PCs with them outside the office, such as putting them on a train shelf or leaving them somewhere unattended, or when they do not keep them in a safe place. However, compared to before the Covid-19 outbreak, more employees are now teleworking. This means that there are more opportunities for PCs to be carried between work and home, hence that much more occasions where the causes of incidents arise.

Loss or theft of paper materials, documents, USB flash drives, and other electronic recording media is related to “Printing confidential information outside the company (at home, satellite offices, etc.)” for the same reason. The main cause of loss and theft remains the same but the availability of printing outside of the office increases the likelihood of forgetting and misplacing such items.

2.1.4. Countermeasures

Based on the hypothesis regarding the relationship between special/exceptional rules and security incidents discussed above, we propose security measures for security incidents. The security measures will also summarize what the related special/exceptional rules should be.

Malware infection on PCs used for telework is closely related to “Using personally owned PCs for work purposes (BYOD),” with the main cause being insufficient security measures compared to company-provided PCs. There are licensing issues when installing company-provided security products on personally-owned PCs. Therefore, it is difficult to strengthen security measures for personally owned PCs, which makes the use of personally owned PCs for work purposes (BYOD) too risky, so it is better to use company-provided PCs. The special/exceptional rules should read: "No exceptions are allowed, use company-provided PCs under all circumstances."

Loss or theft of PCs used for telework is related to "Taking home company-provided PCs that can store confidential information." However, since the main cause has not changed since before the Covid-19 outbreak and the most important issue is information leakage after loss or theft, the special/exceptional rules should read: "Allow the use of company-provided PCs with security measures that take into account the risks ranging from loss or theft to information leakage." In this case, creating special/exceptional rules is not sufficient, but the

rules and procedures should be organized and approved. Specifically, with a focus on information leakage after loss or theft, an environment should be created in which “terminals can be reset to factory settings through remote access after loss or theft,” and a procedure should be established for performing this after the loss or theft.

When we were hastily switching to a telework-centered work style, we needed special/exceptional rules. However, the addition of special/exceptional rules on a temporary basis relaxes the restrictions and regulations established as security measures, thereby weakening the security measures themselves. As this is a temporary measure, the special/exceptional rules should have an expiration date. In addition, when it is time to review internal security rules and reconfirm compliance, the special/exceptional rules should be abolished, or all of the security rules should be updated after analyzing the risks of the special/exceptional rules and adding security measures to address security problems, instead of just keeping the special/exceptional rules in place.

2.1.5. Telework at NTT DATA

The risk of PC loss or theft during telework can be countered by using thin client terminals. However, they must always maintain a communication line to work through remote access, and cannot be used in environments where a communication line cannot be maintained. From the user's perspective, thin client terminals are not an environment that offers high availability, i.e., being usable anytime, anywhere. After all, fat client terminals are superior in terms of availability.

NTT DATA has been enhancing telework since before the Covid-19 outbreak and is using a more secure fat client terminal called Secure FAT. As an example, here is our telework environment based on the concept of zero trust. (Fig. 2-1)

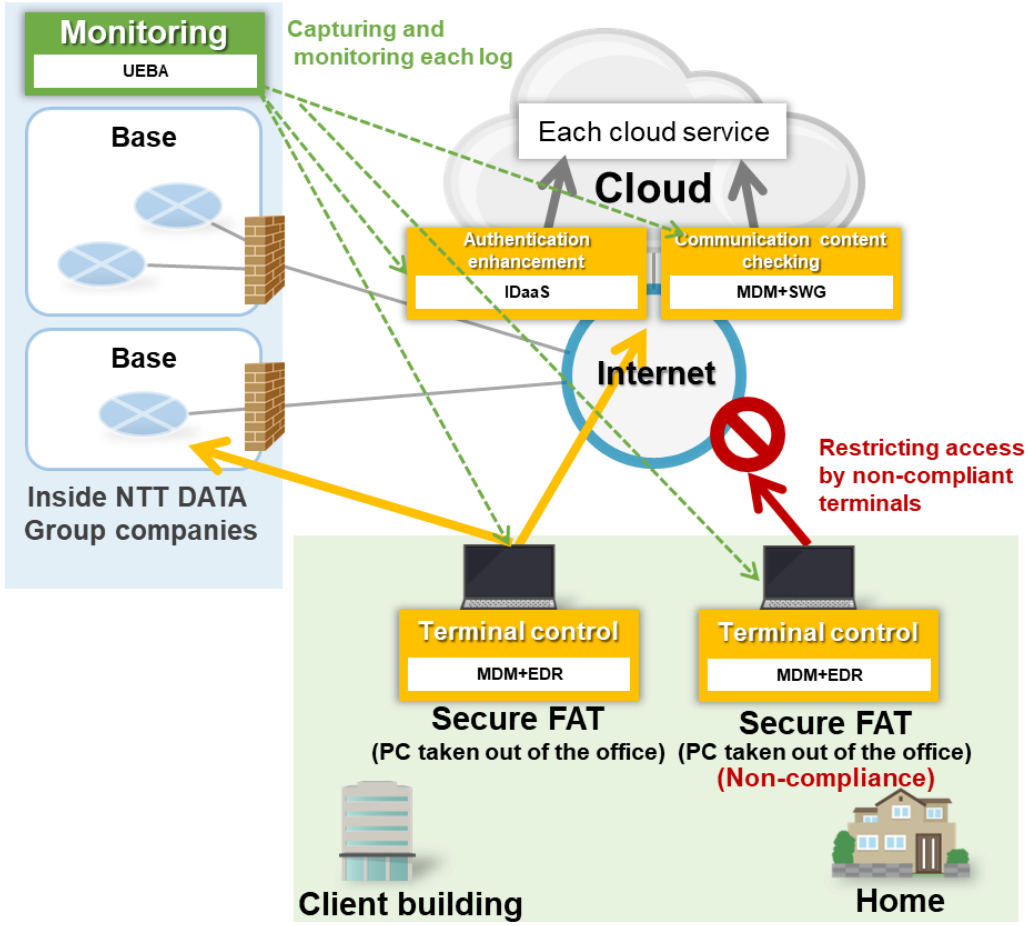


Fig. 2-1: Diagram of telework configuration at NTT DATA

The key elemental technologies are as follows.

- Secure FAT maintains a healthy state by automatically applying patches through centralized management, detecting and blocking malware and cyberattacks. This is a countermeasure for one of the incidents mentioned in 2.1.3: “Malware infection on PCs used for telework (common to both client companies and contractors).” The following elemental technologies are used.
    - MDM (Mobile Device Management):
      It automatically checks the OS and app versions of Secure FAT and applies patches. It allows centralized management by administrators from the management console (SaaS).
    - EDR (Endpoint Detection and Response):
      It monitors the operation and behavior of Secure FAT in real-time to detect malware infections and cyberattacks, and enables automatic handling or remote handling by the administrators. APT attacks and advanced malware infections can also be detected. Forensic personnel can perform detailed investigation and malware removal from the management console (SaaS).
- When communicating from the Secure FAT to cloud services on the Internet or NTT DATA's internal resources, users and the Secure FAT are identified and authenticated, and all communications are protected by detailed permission/control. Identification/authentication prevents the risk of third parties exploiting the PCs for unauthorized access to internal resources after “Loss or theft of PCs used for telework (client companies).” Communication permission/control is a countermeasure for “Malware infection on PCs used for telework (common to both client companies and contractors).” The following elemental technologies are used.
    - IDaaS (Identity as a Service):
      It centralizes ID management and provides unified authentication by linking IDs when accessing cloud services or NTT DATA internal resources from the secure FAT. It also provides single sign-on and multi-factor authentication functions.
    - MDM＋SWG (Secure Web Gateway):
      It is a cloud-based proxy that controls communications from Secure FAT to cloud services or NTT DATA internal resources by encrypting transmissions and checking the contents of communications according to a policy. It blocks dangerous communications related to cyberattacks or malware, as well as communications that violate the policy. In conjunction with MDM, it identifies PCs that do not have the latest OS patches applied, and blocks communications to cloud services and NTT DATA internal resources until the condition improves. Communication content can be monitored by decrypting SSL communication.
    - MDM:
      If the Secure FAT is lost, stolen, or has not been used for a long period of time, the administrator will forcibly initialize (remote wipe) the Secure FAT from the management console (SaaS).
    - UEBA (User and Entity Behavior Analytics):
      It aggregates and monitors the logs of IDaaS, SWG, cloud services, EDR, and Secure FAT to detect cyberattacks based on abnormal behavior of users or devices. Machine learning is used to create supervised models of behavior. As abnormal behavior of users or devices accumulates, the risk score increases and it is detected as a risk, such as a cyberattack.

2.1.6. Conclusion

The special/exceptional rules that have been identified as a problem in this article are measures taken out of necessity in order to hastily switch to a telework-centered work style, knowing that they would create holes in the company's internal security rules. However, the three types of security incidents introduced

in 2.1.3, which occurred frequently under the Covid-19 pandemic, are by no means unpreventable security incidents. There are various security measures that can prevent incidents or mitigate damage. In particular, we believe that many organizations have switched from conventional perimeter defense-based security measures to security measures based on the zero-trust concept in response to the need to establish a safe telework environment during the Covid-19 pandemic. It is important to build a secure work environment using the latest measures and technologies.

We, at NTT DATA, also experienced a breakthrough in security measures from conventional perimeter defense-based security measures to zero-trust security measures, and have been able to accumulate know-how in construction and operation. We believe that we can provide you some tips for building a telework environment based on the zero-trust concept, if you are wondering, "We don't understand what zero trust is," "What should we prepare?" or "What standards should we set?" Let's work together to build a great telework environment.

3. Featured topic, "Revisiting the revision of the Personal Information Protection Act"

3.1. Revised Personal Information Protection Act fully enforced in 2022

The Personal Information Protection Act is reviewed every three years, and the revised Personal Information Protection Act of 2020 went into effect in April 2022. The revision this time aims to reflect the following points [1].

- Protection of individual rights and enhanced use of data
- Addressing new risks associated with the increased cross-border data distribution
- Responding to the era of AI and big data

Table 3-1 provides an overview of the revised Personal Information Protection Act that came into effect in 2022 [2].

Table 3-1: Overview of the revisions

Categories	Revisions
(i) Individual rights	1. Inclusion of short-term retained data in retained personal data 2. Relaxation of individual claims for suspension of use and deletion of personal data and prohibition of provision of personal data to third parties 3. Designation of disclosure methods, including disclosure of electromagnetic records of personal data (digitization) 4. Individual request for disclosure of records provided to third parties 5. Limiting the scope of personal data that can be provided to third parties through opt-out provisions
(ii) Responsibilities that businesses must adhere to	1. Mandatory reporting to the Personal Information Protection Commission and notification to the individual 2. Prohibition of the use of personal information in an improper manner
(iii) Framework to encourage voluntary efforts by businesses	1. Establishment of a new accreditation system for organizations, targeting specific fields (divisions) of a company, under the Accredited Personal Information Protection Organization System
(iv) Data utilization	1. Creation of "pseudonymized information" 2. Obligation to confirm when data is expected to become personal data at the recipient

(v) Penalties	1. Increased fines for offenders violating orders, making false reports, etc. (Maximum fines increased higher for corporations than for offenders.)
(vi) Extraterritorial application of the law and cross-border data transfers	1. Foreign businesses that handle information on individuals in Japan are added to the list of those subject to report collection and orders with penalties 2. Enhancement of information provision to the individual regarding the handling of personal information at the destination when personal information is provided to a third party in a foreign country

3.2. Points to be noted by the businesses

3.2.1. Obligation to report and notify in case of personal data breach

Among the revisions outlined in Table 3-1, attention to “(ii) Responsibilities that businesses must adhere to” has been increasing year after year. In this revision, with "1. Increased fines for offenders violating orders, making false reports, etc." in "(v) Penalties", businesses will need to be acutely aware of "1. Mandatory reporting to the Personal Information Protection Commission and notification to the individual" in "(ii) Responsibilities that businesses must adhere to."

(1) Details of obligation to report and notify in case of data breach [3]

In case of personal data breach, businesses had been obligated to strive to report to the Personal Information Protection Commission and notify the affected individuals, but the revision has made reporting and notification an obligation in the following four cases.

(a) Breach, etc., of personal data containing special care-required personal information
(b) Breach, etc., of personal data that may cause property damage through improper use
(c) Breach, etc. of personal data that may have been conducted for wrongful purposes
(d) Breach, etc. of personal data pertaining to more than 1,000 individuals

Fig. 3-1 summarizes the differences in reporting before and after the revision [4].

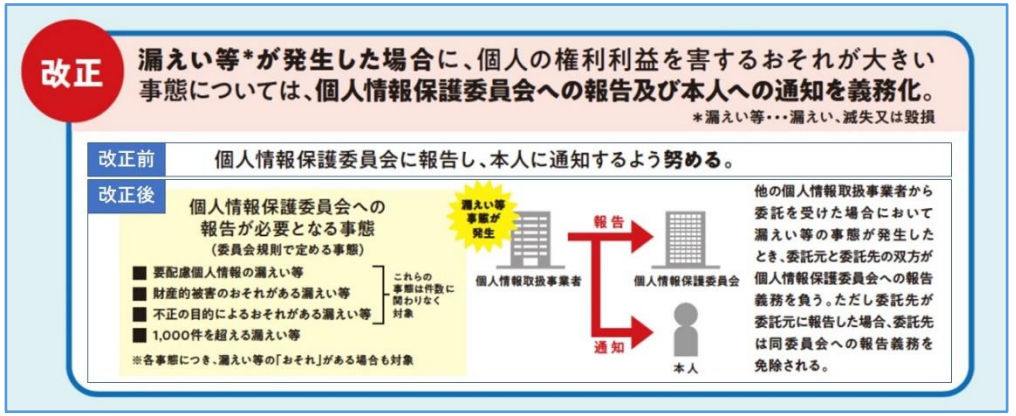


Fig. 3-1: Revisions to reporting and notification obligation

In addition, the Enforcement Regulations of the Personal Information Protection Act establish two types of reports to the Personal Information Protection Commission: "preliminary report" and "final report." As shown in Table 3-2, the reporting deadlines are different for the preliminary report and the final report. In

a preliminary report, the information known at the time of the report concerning the items (i) through (ix) in Table 3-2 are to be reported.

Table 3-2: Reporting and notification

Required actions		Deadlines	Reporting (notification) details
Reporting to the Personal Information Protection Commission	Preliminary report	Immediately upon becoming aware of a situation that is a subject of a report (Approximately within 3-5 days)	(i) Outline, (ii) items of personal data that have been or may have been leaked, (iii) number of individuals whose personal data have been or may have been leaked, (iv) cause, (v) presence or absence of secondary damage or threat thereof, and the details thereof, (vi) status of response to individuals, (vii) status of public disclosure, (viii) measures to prevent recurrence, (ix) other matters that may be of reference (A preliminary report should contain information known at the time of the report concerning the above.)
	Final report	Within 30 days (Within 60 days if there is a possibility of personal data breach for wrongful purposes)	
Notification to the individuals		Immediately, according to the circumstances of the situation (To be determined by taking into consideration the state of understanding, the probability that the rights and interests of the individual will be protected, and any adverse effects that may result from the notification, etc.)	The following among the items to be reported: (i) Outline, (ii) items of personal data that have been or may have been leaked, (iv) cause, (v) presence or absence of secondary damage or threat thereof, and the details thereof, (ix) other matters that may be of reference

(2) Disclosure and reporting of personal data breaches

According to a survey of incidents of personal data breaches and losses conducted by Tokyo Shoko Research, the number of incidents of personal data breaches and losses disclosed by listed companies and their subsidiaries rose from 137 in 2021 to 165 in 2022, and the number of listed companies and their subsidiaries that disclosed such incidents rose from 120 in 2021 to 150 in 2022, both record highs for the second year in a row [5]. In terms of causes of personal data breaches, "virus infection or unauthorized access" accounted for 55.1%, which is also higher than in 2021 (49.6%). If a personal data breach is caused by "virus infection or unauthorized access," it falls under "(c) Breach, etc. of personal data that may have been conducted for wrongful purposes," which requires reporting, so the Personal Information Protection Commission must be informed.

According to its activity report for the first half of FY2022, the Personal Information Protection Commission received 1,587 reports of personal data breach incidents during the same period, about three times as many as it had received a year earlier [6]. Compared to the 1.2-fold increase in the number of disclosed incidents of personal data breaches and losses, the number of reports in the first half of FY2022 has shown a significant increase, growing threefold. The Commission's report states that this is due not only to an increase in the number of incidents of personal data breaches and losses, but also to the revision of the Personal Information Protection Act, which imposed an obligation to report to the Personal Information Protection Commission starting in FY2022, leading to the reporting of incidents of personal data breaches and losses that would have been overlooked in the past. In addition, we believe that the increased attention paid to the protection of personal information in recent years and the "1. Increased fines for offenders violating orders, making false reports, etc." in "(v) Penalties" have also had an impact on this result.

(3) Situation of SMEs

In addition to the increase in the number of reported incidents of personal data breaches and losses, another concern is that not all of the incidents of personal data breaches and losses that are subject to reporting are being properly reported to the Personal Information Protection Commission. According to a survey conducted by the Personal Information Protection Commission, even as of June 2022, after the enforcement of the revised Personal Information Protection Act, nearly 40% of the small and medium-sized enterprises (SMEs) were "unaware" of the revised Act, and three out of four companies were not aware of their obligation to report incidents of personal data breaches [7]. Hospitals and pharmacies often handle special care-required personal information, and many of them are SMEs, so we expect that the number of personal data breach/loss incidents that should have been reported is even higher than 1,587, the number of incidents that were actually reported to the Personal Information Protection Commission.

According to Tokyo Shoko Research's survey of incidents of personal data breaches and losses [5], more than 70% of the listed companies that disclosed personal data breaches were listed on the TSE Prime. The survey also suggests that large companies, which have a wide range of businesses and many employees and customers, are more likely to be involved in cybercrime, but they also have more disclosures due to their well-established governance structures and thorough information disclosure flows. In this respect, we expect that simple loss incidents are more common among SMEs than among large companies, since both the total number of enterprises and the total number of employees are larger in SMEs [8]. However, it is a fact that the number of disclosures of personal data breaches is extremely skewed toward large companies, which suggests that large companies have well-established governance structures and thorough information disclosure flows.

Table 3-3 summarizes the number of disclosures and reports on personal data breaches mentioned above. Based on the difference in the increase in the number of disclosures and reports of personal data breaches as shown in Table 3-3, the fact that three out of four SMEs are not aware of their obligation to report breaches, and the assumption that governance and information disclosure flows are less organized in SMEs than in large companies, we believe that more personal data breaches are occurring in SMEs than reported.

The revised Personal Information Protection Act includes new processes for reporting to the Personal Information Protection Commission and notifying the individual. SMEs are also required to grasp the details of the revision from the Personal Information Protection Commission's web page and organize their flows and processes for handling personal data breaches as necessary. In addition, even if your company has already properly implemented personal information management and operational flow in accordance with the revision of the Personal

Information Protection Act, make sure that your contractors and affiliated SMEs have also appropriately completed their responses to the revision.

Table 3-3: Facts of disclosure and reporting

Subject organizations	Number of subjects	2021	2022	Increase rate
Listed companies and their subsidiaries	No. of disclosures of personal data breach/loss incidents	137 (120 companies)	167 (150 companies)	1.21 times (1.25 times)
Privately owned businesses	No. of personal data breach incidents reported to the Personal Information Protection Commission in the first half of the year	517	**1,587**	**3.07 times**

No. of reports are for the first half of the year only.

3.2.2. Cross-border data transfers

The "(vi) Extraterritorial application of the law and cross-border data transfers" in Table 3-1 is also a point to be noted, as there was controversy over the handling of personal information by LINE Corporation at its overseas offices after the 2020 revision.

The points to note regarding cross-border data transfers in relation to this revision are explained in detail in the Quarterly Report for the fourth quarter of FY2020 [9]. First, businesses that handle personal information need to understand the revisions described in "2. Enhancement of information provision to the individual when personal information is provided to a third party in a foreign country" under "(vi) Extraterritorial application of the law and cross-border data transfers" in Table 3-2. Next, before providing personal data to third parties outside of Japan, businesses need to put in place flows and processes for informing individuals about the handling of their personal data in an easy-to-understand manner in accordance with laws and regulations. These steps are essential for businesses to gain the trust of users.

3.2.3. Other responses

In addition to the reporting and notification in the event of a data breach and the cross-border transfers described in 3.2.1 and 3.2.2, there are other areas where new actions need to be taken as a result of the revision. Required actions range from addressing difficult issues, such as fundamentally reconfirming the way data is used as shown in Tasks 1 to 3 of Fig. 3-2, to simple tasks such as adding items to the current flows and processes.

For example, in "1. Inclusion of short-term retained data in retained personal data" under "(i) Individual rights," the definition of retained personal data has been revised, so it is necessary to check whether any of the data currently handled falls under the category of retained personal data, as shown in Task 1 of Fig. 3-2. If any data is newly classified as retained personal data, it will be necessary to review the operational flows and processes related to the data that is newly classified as retained personal data, as shown in the following Tasks 2 and 3.

On the other hand, for "(3) Designation of disclosure methods, including disclosure of electromagnetic records of personal data (digitization)" in "(i) Individual rights," we believe that although it is necessary to consider how to provide personal data in an electromagnetic manner, in many cases it is only necessary to add new confirmation items to the flow of the current disclosure method.

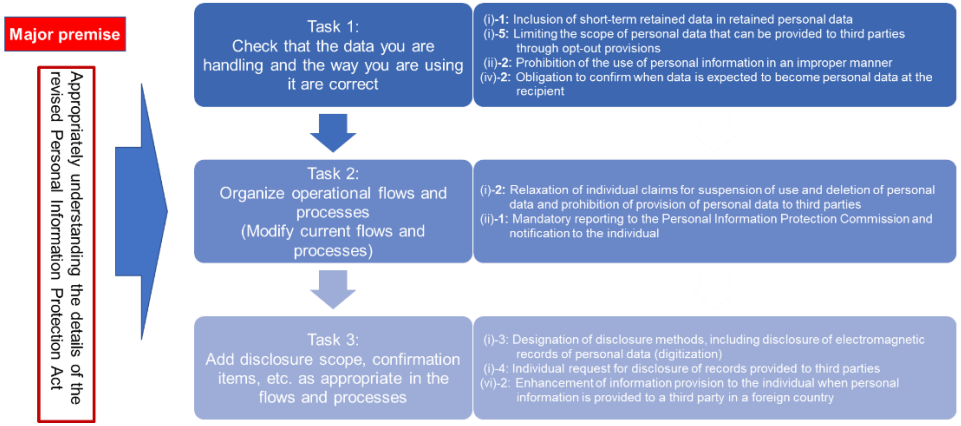


Fig. 3-2: Response to the revision

Even if the operational flows and processes are fine now, if they have not been reviewed for many years, there is a possibility that the current operational flows will become illegal after a legal revision. Naturally, to stay on top of revisions, it is important to keep in mind that the Personal Information Protection Act is subject to change on a regular basis. Since the law is not revised frequently, it is effective if you just set up a process to check the public announcement of revision of the Personal Information Protection Act once a year. The Personal Information Protection Commission's website includes a support page for SMEs that summarizes the revisions to the Personal Information Protection Act [10]. We believe it is important to use this to keep abreast of revisions to the Personal Information Protection Act. In addition, if your company already has a system in place to regularly check revisions to the Personal Information Protection Act and regularly review the operational flows of personal information, it would be reassuring if the scope of the system could be expanded to the entire supply chain to ensure that contractors, affiliated companies and all the other parties that handle personal information are also taking appropriate steps.

3.3. Revision of the Personal Information Protection Act and review of its operation

Even after the 2020 revision of the Personal Information Protection Act took effect, many incidents of personal data breaches occurred, attracting attention in the news and other media. While some incidents caused a stir, such as the loss of a USB flash drive in a project by Amagasaki City [11], new ways of utilizing information were also reported, as in the case of information banks [12]. We believe that the Personal Information Protection Act will continue to be revised in response to incidents and technological developments.

There are no businesses that do not handle personal information at all. It is not enough to just create operational flows and processes related to personal information. This is because the technology and society surrounding personal information will continue to change, and to keep pace with these changes, the Personal Information Protection Act will need to be revised every three years.

It is of course important for businesses to regularly review their rules and procedures in accordance with revisions to the Personal Information Protection Act. In addition, as with the Personal Information Protection Act, businesses need to review how they handle personal information to optimize it for the times, according to technological advances and social conditions.

4. Vulnerability, "MFA fatigue attacks exploiting a multi-factor authentication vulnerability"

Uber Technologies Inc., a company well-known for its ride-sharing and food delivery services, announced in September 2022 that it had suffered a security breach [13]. According to the company's official website, the attacker infiltrated the company's internal systems by compromising multi-factor authentication (MFA) through an "MFA fatigue attack."

In fact, in recent years, several major corporations have suffered similar attacks, which indicates that the use of MFA does not necessarily guarantee safety and security. This article provides an overview of MFA fatigue attacks and how to counter them.

4.1. Overview of MFA

First, we will provide a brief description of the MFA. If you are already familiar with MFA, you may skip this section.

4.1.1. What is MFA?

When you try to log in to a PC or a website, the system checks to see if the person attempting to log in is really you or someone impersonating you. This is called "authentication," and generally uses the following three factors:

(i) Knowledge: Passwords, PINs, etc.
(ii) Possessions: IC cards, One-Time Password (OTP) generators, etc.
(iii) Biometrics: Fingerprints, veins, face, etc.

Of these, Factor (i) passwords are the most widely used by various systems, but problems have been pointed out as attackers succeed in authentication because of the use of weak passwords or the use of the same passwords in different applications. Unfortunately, there is no factor that can achieve perfect authentication without risk, as Factor (ii) possessions can be stolen and Factor (iii) biometrics cannot completely eliminate false recognition.

Then, why not combine multiple factors to increase safety? The MFA method was born out of this idea. In other words, authentication that uses two or more of the three factors mentioned earlier is called MFA. Authentication using two factors is also called two-factor authentication. Authenticating through two rounds with the same type of factors, such as a first password and a second password, is called two-step verification, and is distinguished from two-factor authentication.

In recent years, authentication using MFA has become common in online banking, and is also gaining popularity in services that handle cashable data, such as loyalty point services. Looking at the enterprise sector, it is reported that as of December 2021, 22% of Azure AD users were using strong authentication features, including MFA, which indicates that MFA is still in the early stages of adoption [14].

4.1.2. Examples of MFA methods

Although simply referred to as MFA, there are a number of methods available by combining different authentication factors. Table 4-1 lists major MFA methods in the order of when they became popular. With Item 1 excluded, Items 2 and 3 were commonly used in the past, but at the time of this report, Items 4 and beyond have been increasingly popular.

Table 4-1: Examples of major MFA methods

Item no.	Factor 1	Factor 2	Combination	Remarks
1	PIN	IC card	Knowledge + Possession	Credit cards and ATMs
2	Password	OTP generator	Knowledge + Possession	
3	Password	SMS	Knowledge + Possession	
4	Password	OTP app	Knowledge + Possession	
5	Password	Push notification	Knowledge + Possession	Target of MFA fatigue attacks
6	Private key	Fingerprint	Possession + Biometrics	An example of FIDO2

4.2. Mechanism and examples of MFA fatigue attacks

MFA is very effective in increasing the security of authentication. However, even MFA does not guarantee absolute security. This section explains the mechanism of MFA fatigue attacks targeting MFA that uses push notifications and introduces cases of damage mainly from Uber's case. Note that MFA fatigue attacks are also referred to as MFA bombing attacks in English-speaking countries.

4.2.1. Attack mechanism

The MFA fatigue attack is a method to make an individual mistakenly authenticate the push notification in Item 5 of Table 4-1 in the previous section. The steps of an MFA fatigue attack are as follows:

(i) The attacker obtains the victim's password somehow.
(ii) The attacker attempts to log into the system using the victim's password.
(iii) The system sends a push notification to the victim.
(iv) The attacker repeats (ii) and (iii) until the victim authorizes the login.
(v) The victim mistakenly allows login.

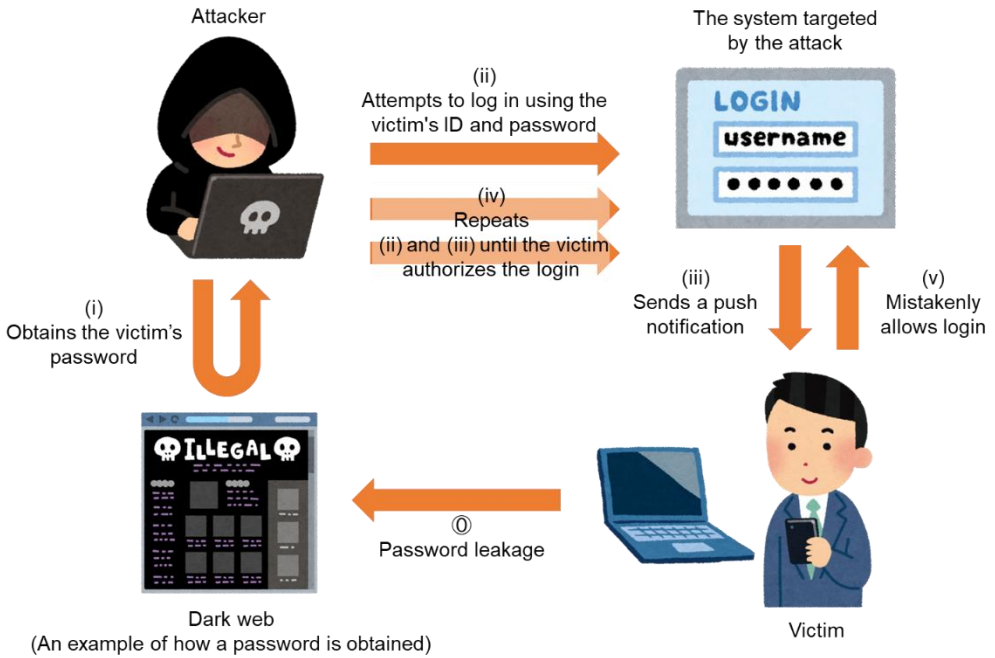


Fig. 4-1: Schematic diagram of an MFA fatigue attack

The name "MFA fatigue attack" comes from the persistent sending of push notifications. Looking at the steps of an MFA fatigue attack again, it is clear that it is an extremely simple attack. If the victim reflexively allows, as they always do, a push notification that appears over and over again, or allows it by mistake, or allows it with a wrong tap position, or allows it after being overwhelmed by a

deluge of notifications, the attacker wins.

4.2.2. Case of attack

The following is a summary of the events that occurred based on the security breach in the MFA fatigue attack announced by Uber on September 19, 2022 [13].

(i) The attacker obtained a password for an account of a contractor for Uber.
(ii) The attacker attempted to log in using the contractor's password.
(iii) The contractor received a push notification, but did not allow login for some time.
(iv) The attacker repeatedly attempted to log in, and eventually the contractor granted access.
(v) The attacker accessed several internal systems of Uber.

We suspect that the password that was obtained by the attacker in (i) had been leaked through a malware infection of the contractor's PC and traded on the dark web. Also, according to some reports, the attacker sent push notifications for over an hour, then posed as someone from the IT department and told the contractor, "If you want to stop the notifications, you have to allow login [15]."

According to Uber's announcement, fortunately the system for commercial services was not affected and internal systems were not severely damaged, but we believe the incident was only one step away from causing service outages or personal data breaches.

Besides Uber, Microsoft and Cisco also reportedly suffered MFA fatigue attacks [16] [17] [18]. The attacks on these three companies are all assumed to have been caused by the cybercrime group “Lapsus$,” and other cyberattacks by Lapsus$ may also be using the MFA fatigue attack.

4.3. Countermeasures against MFA fatigue attacks

This section describes countermeasures against MFA fatigue attacks in two parts: technical countermeasures and organizational/human countermeasures.

4.3.1. Technical countermeasures

As explained in the previous section, the MFA fatigue attack requires the password authentication to have already been compromised. Therefore, protecting passwords is naturally crucial, but this is not limited to MFA fatigue attacks, so we will omit it in this article. One thing to note, however, is that in the event of an MFA fatigue attack, passwords must be reset immediately because they have been leaked. Consider resetting not only the victim's password, but also the passwords of all employees if the cause and scope of the breach cannot be determined.

Now, what technical countermeasures can be taken against MFA fatigue attacks? There are two countermeasures: one is to switch from push notifications to other methods, and the other is to improve push notifications.

First, let’s look at switching from push notifications to other methods. This is an essential countermeasure against MFA fatigue attacks. However, it is time-consuming and costly, as users need to be informed of new operation procedures, and in some cases, the system needs to be modified. Additionally, push notifications provide an excellent user experience, so changing to other methods may cause user dissatisfaction. For example, switching to an OTP app, listed as Item 4 in Table 4-1, requires users to launch the appropriate app and enter a six-digit number, which would add to the hassle. FIDO2 (WebAuthn), which is expected to become more widely used in the future, is not only immune to MFA fatigue attacks, but also offers phishing resistance that is not available in push notifications or OTP apps, and a better user experience. The environments in

which it can be used are expanding, so it is recommended to consider it as an option.

The next is the improvement of push notifications. A major factor behind the success of MFA fatigue attacks is that just by the attacker unilaterally generating push notifications, the user (victim) may mistakenly authorize login thinking that the notifications are for their own authentication. Therefore, the most effective countermeasure is to use a feature called "number matching [19]." This feature displays a number on the screen of the party attempting to log in, and requires the user who has received the push notification to enter that number on their screen when allowing login (see Fig. 4-2). When the user receives the push notification generated by the attacker, the user does not know what number to enter, and therefore cannot allow login. As of this writing, Microsoft has stated that this feature will be automatically applied to all Azure AD users starting February 27, 2023 [20]. Similar features are available from other companies as well as Microsoft, such as Okta's Number Challenge and Cisco's Verified Duo Push. Please note, however, that at the time of this writing, users have to choose from the three numbers displayed in the Number Challenge, so if a user presses a number at random, there is a 1/3 chance that the login will be allowed.

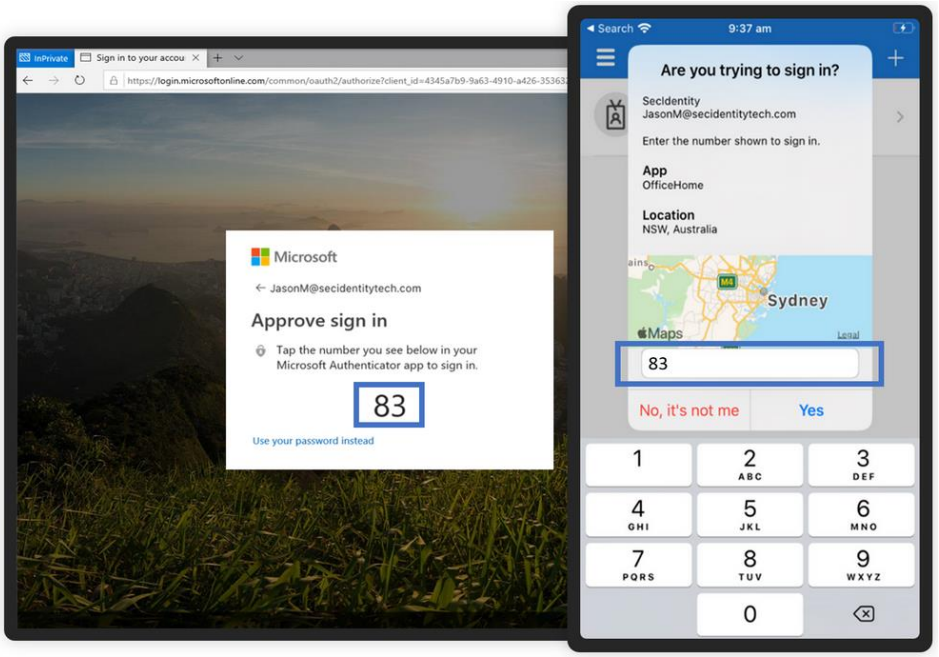


Fig. 4-2: Example of number matching (taken from Microsoft's blog [21])

While number matching can reduce the probability of a successful MFA fatigue attack, it will not stop users from receiving repeated push notifications. In addition to number matching, basic security measures for IDs would be necessary, such as account locking after a certain number of consecutive authentication failures and security features provided by IDaaS and authentication services, e.g., Azure AD Identity Protection.

4.3.2. Organizational/human countermeasures

The vulnerabilities exploited by MFA fatigue attacks are human attention, patience, and normalcy bias, which are commonly associated with social engineering. Therefore, it is important to thoroughly inform users of the following:

(i) The existence of an attack method called MFA fatigue attack
(ii) Never allow login for push notifications that the user does not recognize.
(iii) Report such notifications to the contact person designated beforehand.
(iv) Even if contacted by someone claiming to be a "system administrator" asking for permission, do not blindly trust them, confirm with the contact person.

If a user reports an MFA fatigue attack, unless the user is mistaken, the attacker is attempting to log in illegally using the correct password. Therefore, the system administrator should immediately have the user change their password, and check to see if a similar event has occurred with other users.

4.4. Conclusion

This article provided an overview of MFA fatigue attacks and countermeasures. Nothing can provide absolute security, and MFA is no exception. Organizations using push notifications should inspect whether their system has resilience against MFA fatigue attacks.

As mentioned in the section on technical countermeasures, many authentication methods that do not suffer from MFA fatigue attacks are vulnerable to phishing attacks, etc. Therefore, we believe that FIDO2 (WebAuthn) is the authentication method with superior security that is realistically easy to adopt at present [22]. When considering authentication methods in the future, FIDO2 will probably be the first candidate for many, not only for countering MFA fatigue attacks but also for overall security.

5. Malware and ransomware, “Advanced methods of infection and detection evasion of malware targeting Linux"

5.1. Malware attacks on Linux

5.1.1. Rapid increase in malware attacks on Linux

Malware attacks targeting Linux are on the rise in the second quarter of FY2022. According to Trend Micro, among malware targeting Linux systems, ransomware attacks increased by about 75% and cryptocurrency-mining malware miners were detected about 145% more in the first half of 2022 compared to a year earlier [23]. This indicates an increase in the number of malware attacks targeting Linux systems for money. The number of newly discovered malware targeting Linux systems has also increased. According to AV-ATLAS malware statistics, the number of new malware variants targeting Linux in the first half of 2022 was 1,687,755, which is about 650% higher than the 226,324 in the first half of 2021 [24]. Meanwhile, the number of new malware variants targeting Windows was 41,435,792 in the first half of 2022, down about 43% from 72,538,050 in the first half of 2021 [24]. The number of new malware variants is still higher for Windows than Linux. However, we suspect that attackers are focusing their attacks on Linux, as the number of new malware variants targeting Linux is increasing while the number of new malware variants targeting Windows is decreasing.

5.1.2. Why is Linux targeted?

The main goal of attackers is to gain money. In fact, as discussed in 5.1.1, malware attacks for monetary gain are on the rise. From an attacker's point of view, they can steal more information and have a larger social impact by threatening companies and organizations by stealing and encrypting data on their servers, such as file servers and web servers, than through stealing and encrypting data in their client machines. The greater the damage to the companies and organizations, the higher the probability of their paying the ransom and the higher the amount of the ransom. Therefore, we believe that attackers often target servers.

OSs used in servers are usually Unix- or Linux-based. In fact, Linux-based OSs are used in approximately 38% of web servers, while Windows-based OSs are used in approximately 20%, meaning that Linux is used about twice as much, and if Unix-based OSs are included, about 80% of web servers use Unix/Linux-based OSs [25] [26]. In addition, since an increasing number of companies are shifting their internal infrastructure including servers from on-premises to the cloud [27], and they often choose Linux for PaaS and IaaS, Linux will continue to account for a high percentage of server OSs in the future [28].

Malware attacks targeting Linux are increasing and we believe this is because attackers often target servers and Linux is often chosen as the OS for servers.

5.1.3. Advanced malware targeting Linux

Malware attacks targeting Linux are on the rise, as mentioned in 5.1. Not only that, but malware targeting Linux has become more advanced. As examples, we introduce Linux-targeting malware "Orbit" and "Shikitega" that were newly

discovered in the second quarter of 2022.

5.2. “Orbit,” a new malware variant that is difficult to detect and remove

Orbit is a Linux-targeting malware discovered and announced by Intezer on July 6, 2022 [29]. It has advanced features to evade detection and removal, and can steal information from infected machines without leaving any traces. In particular, the methods used to achieve persistence, so that Orbit would be automatically activated even after machine reboot, and to make Orbit difficult to remove, are advanced and different from those used in conventional malware. Based on Intezer's analysis [29], we will look at Orbit's behavior, which shows the advanced nature of malware targeting Linux.

(1) Infection mechanism

In order to achieve persistence of Orbit, administrator privileges are required. Persistence means that the malware is configured to be automatically launched even after the machine is rebooted. Therefore, for Orbit infection, the attacker illegally logs into a target Linux machine with an account that has administrative privileges in a brute force attack, social engineering attack, or phishing attack [30]. After the unauthorized login, the attacker persistently infects the system with Orbit in the following steps (Fig. 5-1).

(i) Dropper execution

At the time of writing, there is no information available on how the Orbit dropper is downloaded onto a machine, but the attacker first downloads the dropper onto the Linux machine somehow and executes it with administrator privileges. At this time, the attacker sets arguments for the dropper to switch the following dropper behaviors:

- Setting Orbit behavior after machine reboot
  - Achieving persistence so that Orbit starts automatically after a machine reboot
  - Or removing Orbit after a machine reboot
- Setting the path where Orbit is installed
- Uninstalling Orbit

(ii) Adding malicious code to shared libraries

When the dropper is activated, it downloads malicious code from the attacker's server. The file format for this malicious code is Shared Object (.so). Shared Object is a file format used for shared libraries. By adding the Shared Object to a shared library by adding it to environment variables or editing configuration files, the Shared Object of malicious code can be loaded at the time of program execution.

(iii) Achieving persistence

In Linux, when a program is launched, it loads shared libraries using the preloading feature before the program starts. Orbit gains persistence using the preloading feature of shared libraries. Orbit uses two separate preloading methods. The first method is to add the path of the shared library containing Orbit to the configuration file used by the loader. The second method is to tamper with the loader itself and load the shared library containing Orbit through a fake configuration file. Thus, if malicious code is added to a shared library, it becomes possible to perform malicious activities such as installing backdoors or stealing information, so Orbit infection is successful at this point.

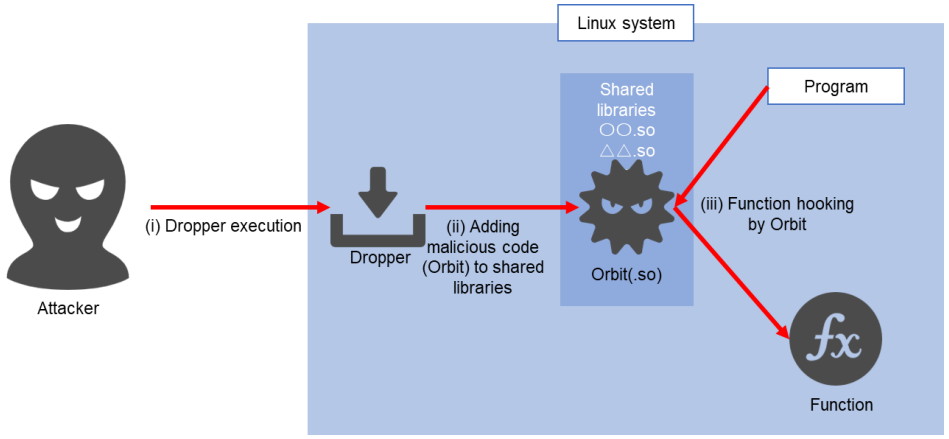


Fig. 5-1: Mechanism of Orbit infection

(2) Attack features

(i) Function hooking

When Orbit starts up, it hooks specific functions in the three libraries, libc, libcap, and Pluggable Authentication Module (PAM), and rewrites the function processes. Be it an existing process or a new process, if it tries to use any of the specific functions in libc, libcap, or PAM, it will use the functions that have been rewritten by Orbit. This function hooking enables Orbit to perform malicious activities such as installing backdoors and stealing information. These will be explained later.

(ii) Backdoor

Let's see what happens when Orbit hooks the PAM library. The PAM library is a library used for user authentication. Orbit hooks three PAM library functions: pam_open_session, pam_authenticate, and pam_acct_mgmt. pam_authenticate is the function used for user authentication. SSH calls pam_authenticate when it performs the authentication process. Orbit checks if the username and password for authenticating the attacker, which are hardcoded in its own binary file, and the credential entered when pam_authenticate is called are the same or not. If they are the same, the port number used for the connection is recorded so that traces of this communication can later be erased from logs, etc., and an SSH connection with the attacker is initiated. The username and password hardcoded into Orbit are known only to the attacker. This means that if an attacker requests a connection to SSH of the Orbit-infected Linux machine, Orbit can allow the connection even if the attacker does not have an account. In other words, the attacker can use SSH as a backdoor to illegally log in to the Orbit-infected Linux machine.

(iii) Theft of SSH credentials

If the credentials entered when calling pam_authenticate are not the same as the hardcoded username and password, Orbit records the credentials and continues the process. Orbit also steals the credentials from remote access to the infected terminal via SSH and provides them to the attacker.

(iv) Data theft from file reading/writing and program execution

In addition, Orbit steals information other than SSH credentials. Orbit hooks two functions, "read" and "write," and obtains data from the hooked functions when processes on the terminal read/write data on the hard disk, etc. In doing so, Orbit refers to the hardcoded sniff_ssh_session flag, and if the flag is false, Orbit logs only the data read/written by processes in sudo or ssh sessions. If the flag is true, Orbit logs all written data without verifying the calling process. Additionally, Orbit hooks the function execve used to execute programs and obtains the full path and execution time of the executable file. When the hooked function execve ends, it returns the return value of execve. If the user executes the program and it does not return a return value or returns a different value than expected, the user may notice an anomaly. Orbit returns a normal return value for the hooked function, to make the program appear to behave normally to the user, preventing them from

noticing the infection. In other words, Orbit steals information on the data read/written by processes and the results of program execution without the user noticing it.

(v) Detection evasion (hiding Orbit-related files)

Orbit avoids detection by hooking various functions and rewriting the processing results, so that its presence is not revealed in log files or running processes. Let's look at some of the features of Orbit's detection evasion.

Orbit may evade detection by hooking the readdir function. The readdir function is a function that reads directories or files. Orbit hooks the readdir function and checks the GID value of the calling process of the readdir function. The GID value refers to the Group ID, which is associated with users, processes, and files and is used for group-based access control. A certain GID value is set for directories, files, and processes related to Orbit so that they can be identified as being related to Orbit. When a process related to Orbit executes the readdir function, Orbit determines that a process with Orbit's GID value has executed the readdir function and outputs a list of all directory and file names that are the return values of the readdir function. When a process not related to Orbit executes the readdir function, Orbit determines that a process with a GID value different from Orbit's GID value has executed the readdir function and removes all directory and file names with Orbit's GID value from the list of all directory and file names to be output as the return values of the readdir function.

As shown in this example, the GID value is used to change the behavior of functions so that information about Orbit is not visible to non-Orbit processes, thereby hiding information that would reveal Orbit's existence.

(vi) Detection evasion (hiding dynamic information such as Orbit processes and communications)

Simply hooking the readdir function to hide Orbit-related directory and file names may not be sufficient, as users may notice Orbit from the traces of Orbit's operation left in standard log files and other files in the system. One approach to address this is to hide all files that contain traces of Orbit's operations, but this would also make standard log files and other files that should be there invisible to the user, potentially arousing their suspicion, and they might then notice Orbit. Therefore, Orbit does not hide the files that include traces of its operations, but instead removes only Orbit-related information from the contents of those files and outputs the remaining information, as shown in

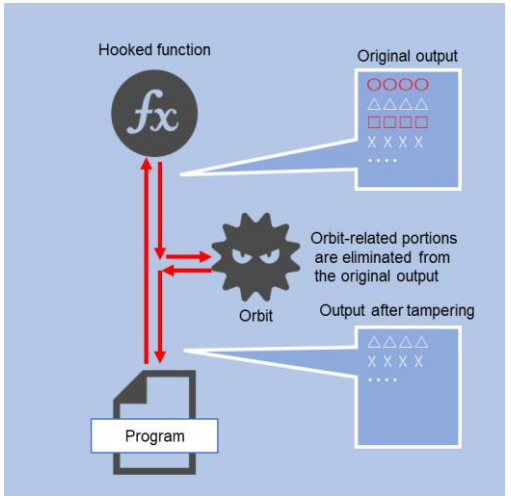


Fig. 5-2. Specifically, Orbit hooks the file opening functions fopen, open, open64, and openat, and checks whether the file that was provided to each of these functions is part of the proc file system. The proc file system stores various information about the system's running processes, memory, hardware, etc. and by referring to files in the proc file system, various information about the system can be obtained [31]. If the provided file is part of the proc file system, Orbit checks the file path and file contents. Then, any information related to Orbit in the file is removed, and the rest of the information is output.

For example, Orbit checks "/proc/net/tcp" which contains TCP connection information. There is a possibility that information about Orbit's installed backdoor communication may remain in the files under this /proc/net/tcp directory, and if the

user sees it, they may notice the existence of the backdoor. Therefore, when the user opens a file under /proc/net/tcp, Orbit performs a process to hide any traces of the backdoor. Specifically, Orbit reads the contents of the opened file under /proc/net/tcp one line at a time and compares them with the port number and address information recorded when the attacker connected to SSH. It then creates a temporary file by deleting the lines containing that information. Finally, Orbit returns the contents of this temporary file that has no traces of the backdoor to the user as the return value. This means that even if the user opens a file under proc/net/tcp, they will not find any traces of the backdoor used by the attacker.

If a user opens files that provide information about CPU usage or the state of processes on the proc file system, Orbit conceals its presence by removing any Orbit-related information from the output of these files in the same manner as described above.

The behavior of the execve function that executes the program is also modified to hide Orbit. For example, when executing commands such as ip or iptables that display information about the network, Orbit-related information is removed from the output of the command.

As explained in (v) and (vi) above, Orbit hooks various functions and removes Orbit-related information from log files and command outputs to conceal its existence, making it difficult to detect. Intezer has reported that no antivirus software was able to detect Orbit when the company tested 60 antivirus software products. This indicates that the detection evasion techniques implemented in Orbit are highly advanced.

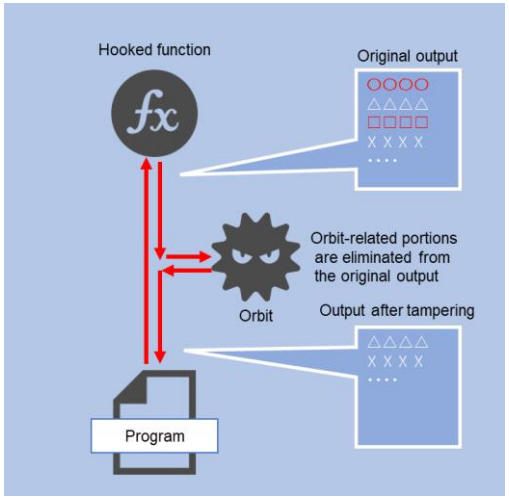


Fig. 5-2: Orbit's detection evasion method

(3) How to achieve persistence

Orbit uses unique methods to achieve persistence and makes removal difficult. The usual method for malware to achieve persistence using a shared library is to preload itself before other libraries by using an environment variable called LD_PRELOAD. Unlike other malware, however, to achieve persistence, Orbit preloads itself by using a configuration file instead of an environment variable. Orbit preloads itself using two unique methods, as described in (iii)Achieving persistence of (1)Infection mechanism. The first method is to add the path of the shared library containing Orbit to the configuration file used by the loader. The second method is to tamper with the loader itself and load the shared library containing Orbit through a fake configuration file. The loader here refers to ld.so and ld-linux.so, the programs in Linux that locate and load the shared libraries needed by a program and prepare it for execution [32].

(i) Achieving persistence by adding a path to the configuration file

This method is to add the path to the shared library containing Orbit to the configuration file "/etc/ld.so.preload" as shown in Fig. 5-3. This causes the loader to load Orbit first. In addition, all new processes will also load Orbit first.

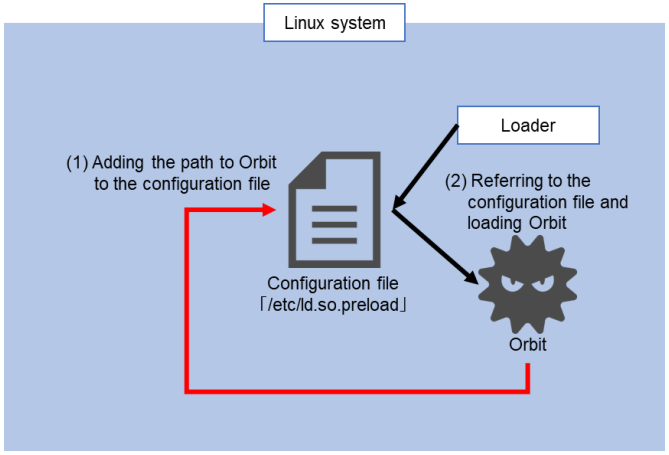


Fig. 5-3: Achieving persistence by adding a path to the configuration file

(ii) Achieving persistence by patching the loader

Orbit first creates a copy of the loader's binary file and makes it possible to apply patches. Then it searches for the string "/etc/ld.so.preload" in the copied binary file and replaces it with the path to a fake configuration file that Orbit has prepared. The fake configuration file contains the path to Orbit. In other words, when the loader is patched as shown in Fig. 5-4, it loads Orbit by referring to the fake configuration file provided by Orbit instead of the original configuration file it should reference, "/etc/ld.so.preload."

The author of Orbit has set up these two methods to complement each other in case one of them is eliminated. For example, if the administrator of a Linux machine infected with Orbit tries to prevent the loading of Orbit by deleting the configuration file "/etc/ld.so.preload," the patched loader will load Orbit. The loaded Orbit will then add the path to Orbit to the configuration file "/etc/ld.so.preload" once again. On the other hand, if the administrator overwrites the tampered loader with the regular loader and returns to using the regular loader, the regular loader will load Orbit since the path to Orbit has been added to the configuration file "/etc/ld.so.preload." The loaded Orbit will then tamper with the loader again.

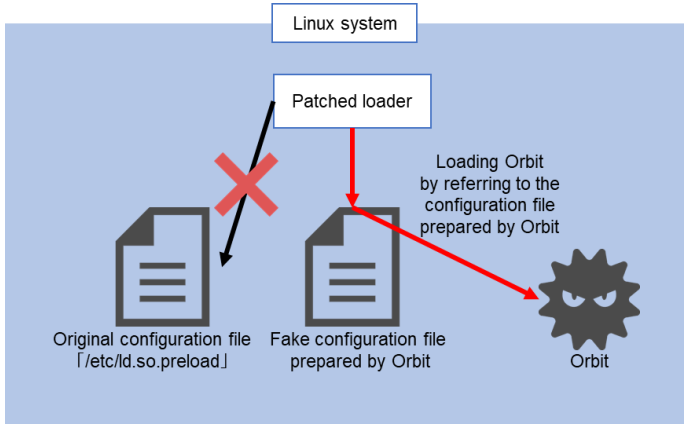


Fig. 5-4: Achieving persistence by patching the loader

5.3. "Shikitega," new malware that is difficult to detect and also targets IoT

Shikitega is a Linux-targeting malware reported by AT&T Alien Labs on September 6, 2022 [33]. It also targets IoT using Linux. Shikitega implements multiple detection evasion techniques, and once it infects a machine, it can seize administrative privileges or use the infected machine's CPU resources for cryptocurrency mining. Orbit was known for its method of evading malware activity detection after infection, but Shikitega is characterized by its method of evading detection before a successful infection. Based on the analysis of AT&T Alien Labs [33], we explain Shikitega's infection mechanism and detection evasion method.

(1) Infection mechanism

To evade detection, Shikitega installs its malicious code gradually so that the entirety of Shikitega's malicious code is not revealed. It divides the installation process up to the final installation of the program in three stages and uses three types of droppers as shown in Fig. 5-5. Each of the three types of droppers is responsible for a different task.

(i) Dropper (i): Downloading and executing Metasploit

Shikitega's first dropper, Dropper (i), is a very small ELF file of about 370 bytes. Dropper (i) downloads and executes Mettle, a module of Metasploit, an open source penetration testing tool. Mettle allows a wide range of attacks, including webcam control, sniffer, shellcode execution, etc. Dropper (i) also uses wget to download Dropper (ii) for the second stage from the C&C server.

(ii) Dropper (ii): Seizing administrative privileges

Dropper (ii) is encrypted with the "Shikata Ga Nai" encoder included in Metasploit to evade detection, and is an ELF file of about 1 kilobyte in encrypted form. To execute the shellcode of Dropper (ii), Shikitega repeatedly decrypts it using "Shikata Ga Nai" until an executable shellcode is obtained. When this shellcode is executed,

it communicates with the C&C server and downloads additional shellcode and files required to seize administrator privileges. The additional shellcode and files are not stored on the hard disk, but are unpacked into memory and then executed to evade detection. This allows Shikitega to exploit two Linux vulnerabilities, CVE-2021-4034 and CVE-2021-3493, to execute commands with administrator privileges. Additionally, the shellcode of Dropper (ii) downloads Dropper (iii).

(iii) Dropper (iii): Executing miner and achieving persistence

Dropper (iii) is also encrypted with "Shikata Ga Nai" to evade detection. Dropper (iii) also repeats decryption until an executable shellcode is obtained. When this shellcode of Dropper (iii) is executed, it communicates with the C&C server and downloads XMRig miner, a Monero cryptocurrency miner, along with its configuration file and five shell scripts (Table 5-1) required for achieving persistence. These shell scripts and files are also executed in memory the same way. By running the downloaded XMRig miner and mining Monero, the attacker can obtain Monero. The XMRig miner persists even after machine restarts. Persistence is achieved by executing the downloaded five shell scripts. Specifically, the following four programs are registered in the cron configuration file by executing the crontab command, which configures cron to automatically execute programs at regular intervals.

- A program to download XMRig miner and its configuration file from the C&C server with the privileges of the logged-in user during the infection
- A program to execute XMRig miner with the privileges of the logged-in user during the infection
- A program to download XMRig miner and its configuration file with administrative privileges
- A program to execute XMRig miner with administrative privileges

This allows continuous download and execution of XMRig miner and its configuration file from the C&C server. If the crontab command does not exist on the Linux machine, Shikitega will install crontab. Once persistence is achieved, continuous mining of Monero can be performed with only the cron configuration, and no other files are required. Therefore, to hide traces of its activity, Shikitega deletes all the downloaded files from the machine after persistence is achieved.

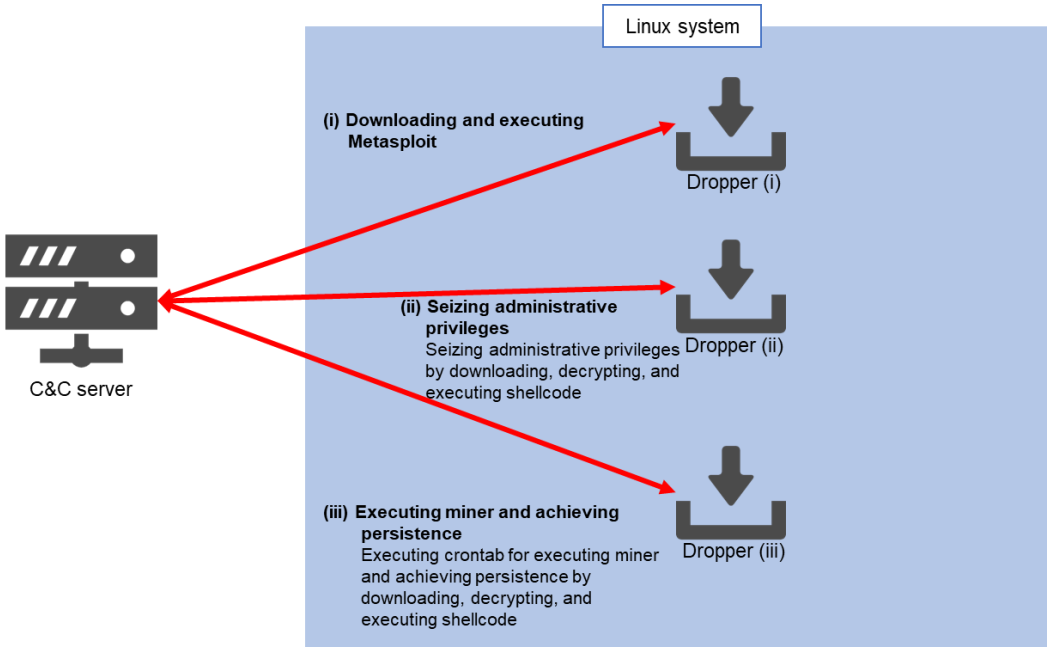


Fig. 5-5: Shikitega infection mechanism

Table 5-1: Shell scripts for achieving persistence

Script name	Action
unix.sh	Check for the presence of crontab command on the Linux machine and install crontab if it does not exist
truct.sh	Register in crontab a program to download XMRig miner and its configuration file from the C&C server with the privileges of the logged-in user during the infection
brict.sh	Register in crontab a program to execute XMRig miner with the privileges of the logged-in user during the infection
restrict.sh	Register in crontab a program to download XMRig miner and its configuration file with administrative privileges
politrict.sh	Register in crontab a program to execute XMRig miner with administrative privileges

(2) Detection evasion methods

Shikitega mainly uses the following three methods to make detection difficult.

(i) Installation of Shikitega by an infection chain

Shikitega does not install the program for infection all at once, but installs it in three separate stages. This method is called an infection chain, which installs an infection program in multiple stages for execution [34]. Using an infection chain can make pattern matching detection by antivirus software more difficult. For example, if malware is executed as a single program, its characteristics will match those of known malware, making it easy to detect through pattern matching. However, if the malware is executed in multiple programs through an infection chain, detection through pattern matching could be avoided. Furthermore, shellcode, shell scripts and files downloaded by the dropper from the C&C server are not stored on the hard disk, but are unpacked into memory and then executed. Many antivirus programs monitor files on the hard disk, which makes detection difficult when malware is executed directly in memory.

(ii) Obfuscation by polymorphic encoding

Shikitega uses "Shikata Ga Nai (No way to avoid)," one of the common encoders used by Metasploit, to obfuscate shellcode, making it difficult for virus protection software to detect through pattern matching. Specifically, "Shikata Ga Nai" uses a polymorphic XOR additive feedback encoder. Polymorphic XOR additive feedback encoders are characterized by the fact that a single shellcode is encrypted multiple times, each time using a different encryption key, resulting in a different output after encryption [35]. This can make pattern matching detection by antivirus software more difficult. Also, by obfuscating the shellcode, static analysis is made difficult. Specifically, even if the shellcode can be retrieved before Shikitega erases the dropper, the contents are encrypted by "Shikata Ga Nai" and are difficult to decrypt, making static analysis of the script impossible.

(iii) C&C servers on legitimate cloud services

Shikitega hosts its C&C servers on legitimate cloud services. Communication from Shikitega to the C&C server may use direct IP addresses instead of domain names and may not use the same IP address for an extended period of time, making it difficult to create an effective IoC. As a result, detecting or blocking communication from Shikitega to the C&C server is not very effective.

5.4. Countermeasures against Orbit and Shikitega

As mentioned in 5.1, there has been an increase in malware targeting Linux, and it is necessary to implement proper malware countermeasures for Linux as well. In addition, as shown in the examples of Orbit and Shikitega in 5.2 and 5.3, malware attacks targeting Linux are becoming more advanced. Therefore, general countermeasures such as installing antivirus software and applying

patches alone may not be sufficient to prevent malware infection. Based on the analysis results of Orbit and Shikitega, we propose the following three countermeasures.

(1) Use of SELinux

Since both Orbit and Shikitega require administrative privileges to execute malicious code, we believe that the use of SELinux, which can restrict administrative privileges, is an effective countermeasure.

(2) Installation of endpoint security products capable of behavior detection

Shikitega uses a polymorphic encoder to obfuscate shellcode, making detection by pattern matching difficult, so we believe that antivirus software alone is not sufficient to detect this type of malware. As a countermeasure against such malware, we believe it is effective to combine the introduction of endpoint security products that can monitor information in the terminal and detect suspicious behavior at the process level. Specifically, some NGAV (Next Generation Anti-Virus) and EDR (Endpoint Detection and Response) products are capable of behavior detection. For example, by using endpoint security products capable of behavior detection, it may be possible to detect rewriting of shared libraries or downloading and executing of Metasploit, a penetration testing tool, as an abnormal behavior, and block the process.

(3) Installation of UEBA

Since Orbit modifies its output so that no trace of its activity can be found, it is difficult to detect it based on information on the machine alone. As a countermeasure for such malware, it is effective to combine the use of UEBA (User and Entity Behavior Analytics) to detect behavior using logs from non-infected machines. For example, it may be possible to detect Orbit infection by combining detection of communication from an Orbit-infected machine to an attacker's server on the Internet, which is not usually accessed, and authentication failure logs due to brute force attacks, based on the above EDR anomaly detection alerts and Firewall logs.

5.5. Conclusion

There has been an increase in the number of malware attacks for monetary purposes targeting Linux-based machines, such as servers in the cloud and IoT devices. In addition, advanced malware that is difficult to detect, such as Orbit and Shikitega, targeting Linux, is increasing. Therefore, it is important to be prepared for malware attacks on Linux, which requires not only conventional countermeasures such as installing antivirus software and applying patches, but also the introduction of endpoint security products and UEBA that are capable of behavior detection in order to counter advanced malware that is difficult to detect. In addition, a multi-layered defense that combines these measures is also necessary. Your organization should also check the status of countermeasures for Linux-based systems and be prepared for such malware attacks.

6. Outlook

Abuse of chatbots for cybercrime

ChatGPT, released by OpenAI at the end of 2022, became a global sensation overnight. This well-performing chatbot returns answers that are so good that it is difficult to tell whether they were written by a human or an AI, and cybercriminals have been intrigued by it.

On the dark web, attackers appear to be exploiting ChatGPT to generate phishing content and to be exchanging ideas about the automatic generation of malware [36]. By using chatbots such as ChatGPT, even individuals with relatively low skill can participate in cyberattacks, and skilled attackers will be able to arm themselves more efficiently. The abuse of chatbots is expected to increase the variety of cyberattacks in the future.

Meanwhile, we predict that the use of AI will expand not only among cybercriminals, but also for those who defend against cyberattacks. AI has been used in several fields, such as detecting malware and abnormal behavior. However, there are few cases where incident response has been fully automated, and most incident response flows include human decision points. Lack of information or experience is a bottleneck for human decision making. AI is good at learning from vast amounts of information and continuing to accumulate experience. In the near future, we will see AI as a consultant to assist human decision making. Further into the future, AI may continue to analyze OSINT and all internal information of an organization, and resolve incidents it discovers in an instant. It will be a test to see how far humans will be able to entrust their decisions to AI, which will continue to make unwavering decisions 24 hours a day, 365 days a year.

Breach of special care-required personal information containing medical information

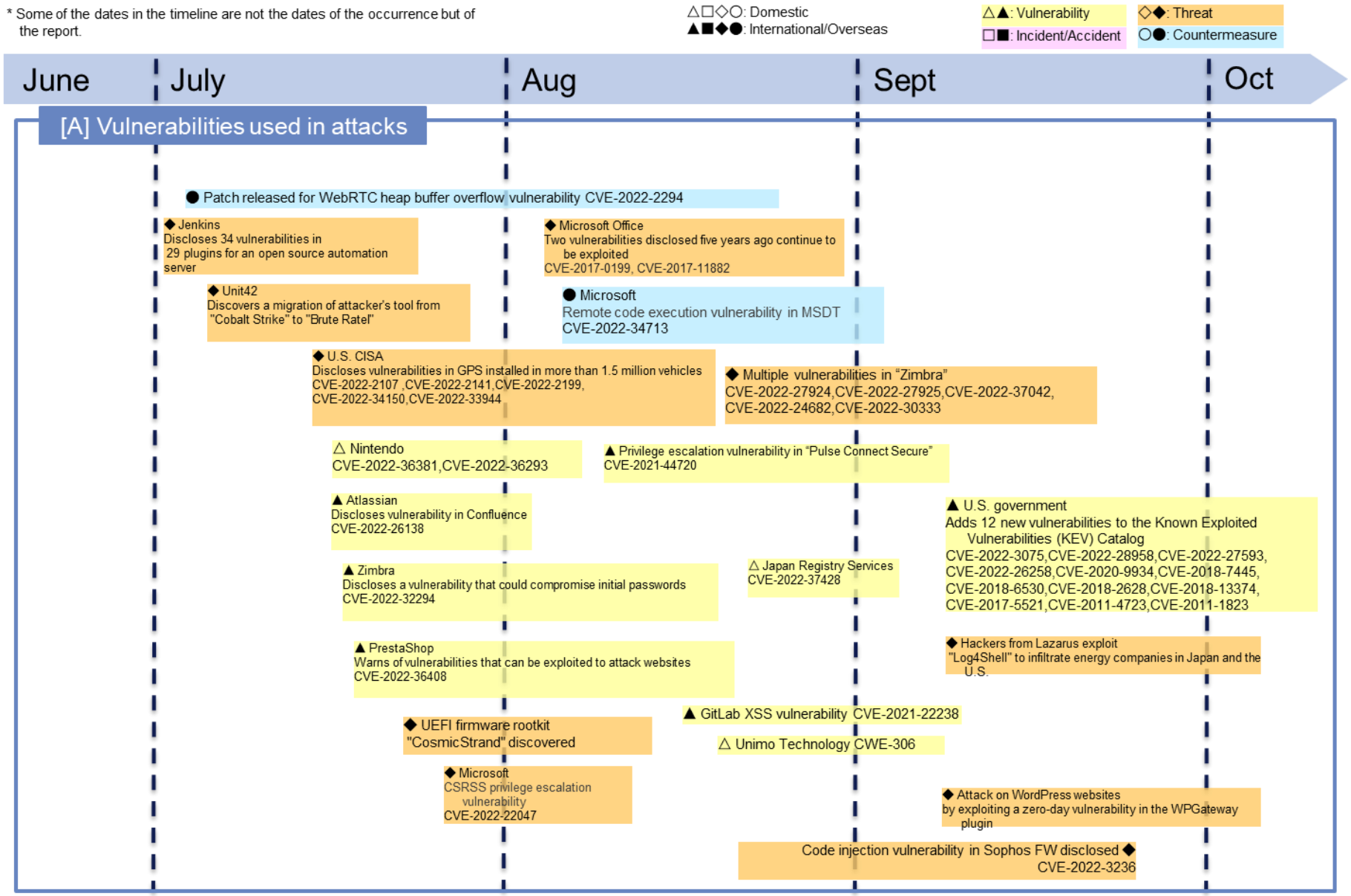
According to the activity report of the Personal Information Protection Commission for the first half of FY2022, which was also mentioned in Chapter 3, the main cause of reported data breaches was "incorrect delivery or loss of documents containing special care-required personal information in hospitals and pharmacies [6]." Personal medical information falls under the category of special care-required personal information. This means that if medical information is leaked, it must be reported to the Personal Information Protection Commission, regardless of the reason or amount of data leaked, due to the importance of the information.

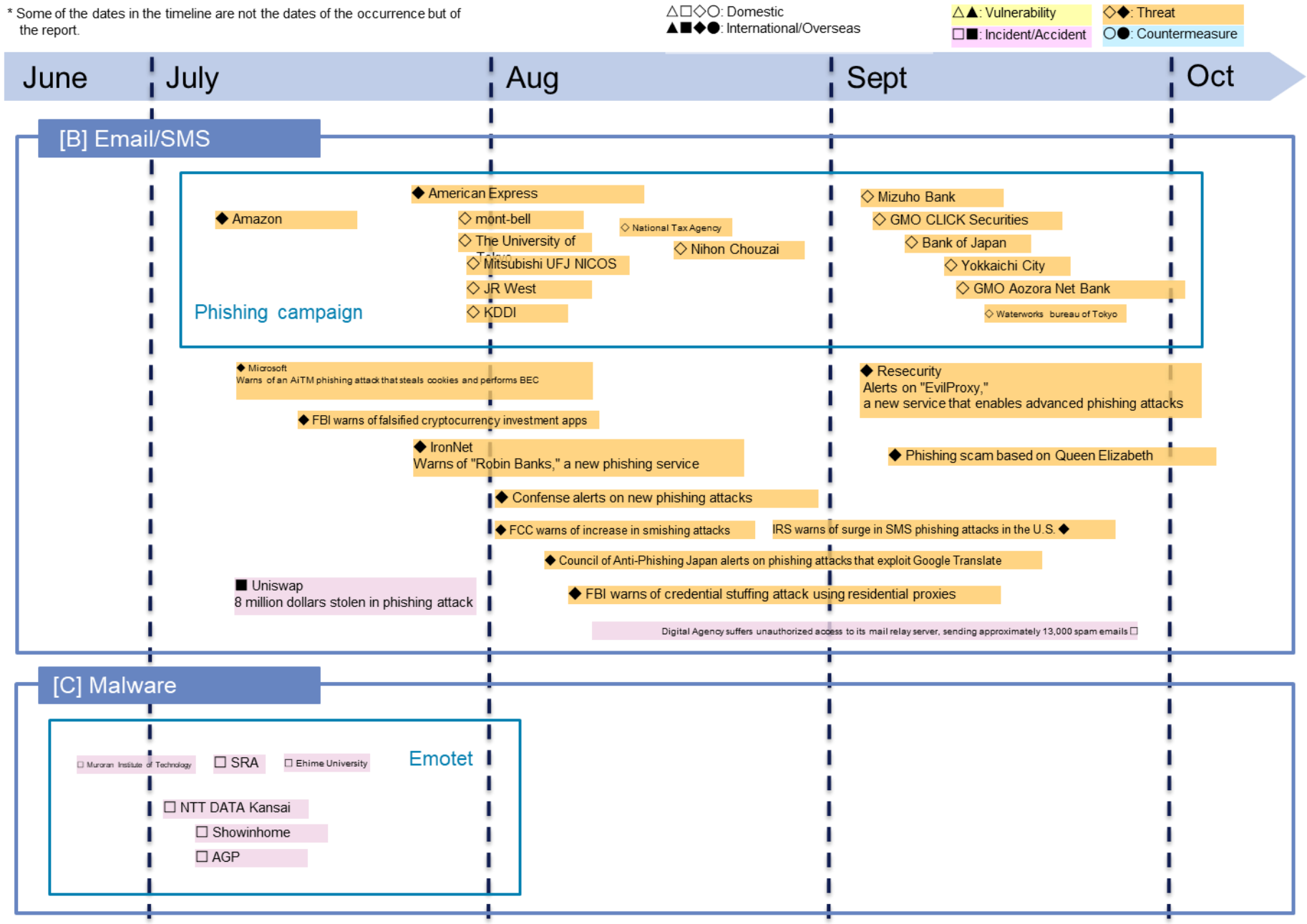
In January 2023, a data breach accident occurred in which a doctor at Kounosu Kyousei Hospital accidentally streamed the audio of a medical examination on a personal smartphone video streaming app [37]. While measures such as education and thorough implementation of rules regarding personal information are important, human errors cannot be completely eliminated. Therefore, it is necessary to take fundamental measures to prevent leaks.

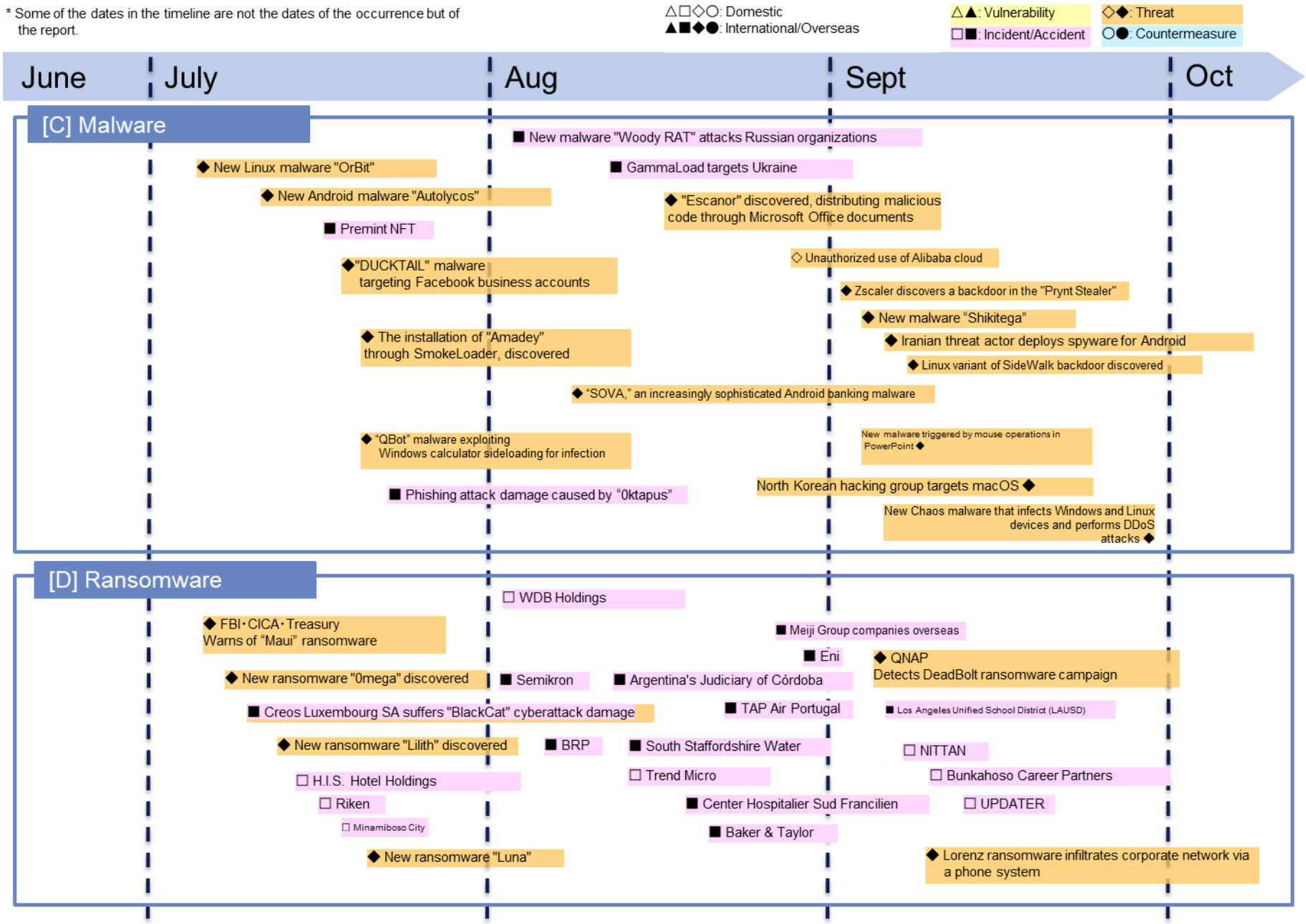
Large companies provide employees with business-only smartphones and prohibit them from bringing their own smartphones into areas where confidential information is handled. Of course, business-only smartphones only have business-related functions and apps installed. The best measure is to control the installation of apps using device management technologies such as MDM, but even separating apps to be installed on personal smartphones and business smartphones based on rules can prevent human errors.

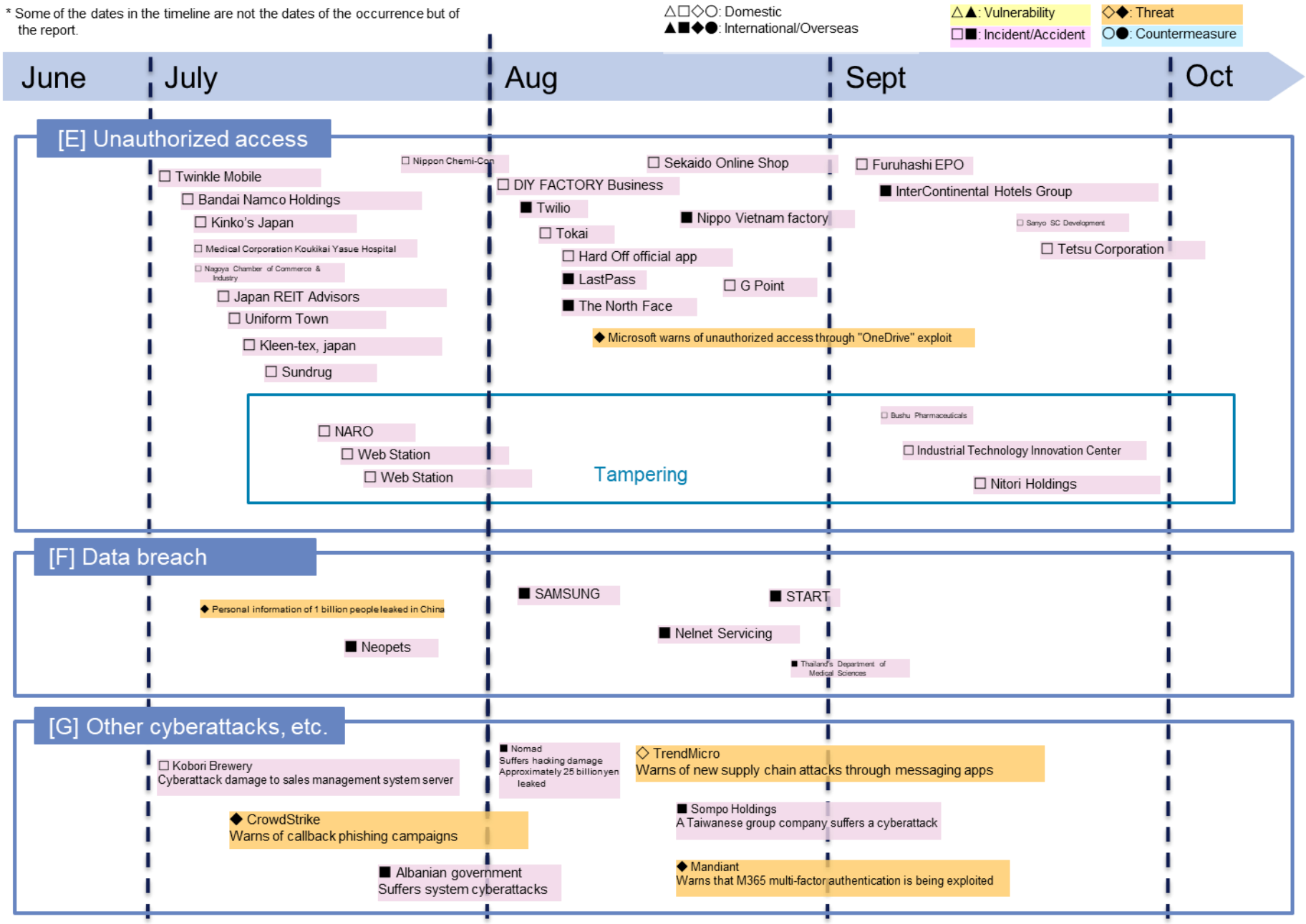
However, in the medical field, it is known that it is difficult to restrict the use of smartphones or limit areas due to immediacy and availability. Furthermore, as hospitals and pharmacies are SMEs, we think that taking systemic measures for personal information will be difficult from a cost perspective. For these reasons, we believe that it will be difficult for SMEs and medical institutions to implement fundamental countermeasures against data breaches through smartphones in a short period of time. Therefore, we are afraid that personal data breaches from hospitals and pharmacies will continue to occur.

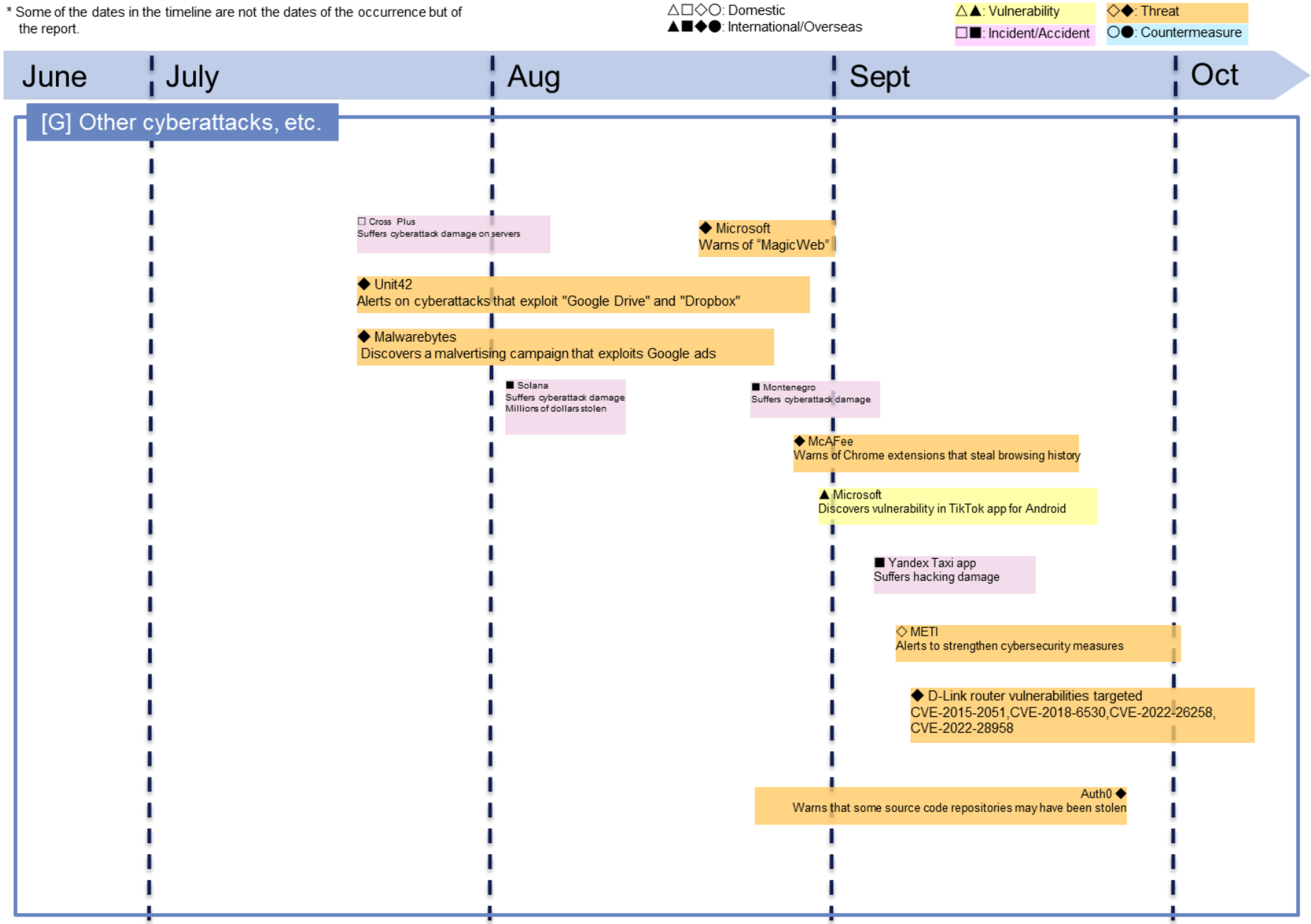
7. Timeline











References

[1] 独立行政法人情報処理推進機構, “情報セキュリティ白書2022,” 1 9 2022. [オンライン]. Available: https://www.ipa.go.jp/files/000100474.pdf.

[2] 個人情報保護委員会, “個人情報の保護に関する法律等の一部を改正する法律（概要）,” [オンライン]. Available: https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf.

[3] 個人情報保護委員会, “個人情報の保護に関する法律についてのガイドライン（通則編）,” 8 9 2022. [オンライン]. Available: https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-5-3.

[4] 個人情報保護委員会, “令和２年改正個人情報保護法概要リーフレット(令和4年2月）,” 4 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/revised_APPI_leaflet2022.pdf.

[5] 株式会社東京商工リサーチ, “個人情報漏えい・紛失事故 2年連続最多を更新 件数は165件、流出・紛失情報は592万人分 ～ 2022年「上場企業の個人情報漏えい・紛失事故」調査 ～,” 19 1 2023. [オンライン]. Available: https://www.tsr-net.co.jp/news/analysis/20230119_01.html.

[6] 個人情報保護委員会, “令和４年度上半期における個人情報保護委員会の活動実績について,” 9 11 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/R4_kamihanki.pdf.

[7] 個人情報保護委員会, “中小規模事業者の安全管理措置に関する実態調査,” 27 6 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/R3_chuushou_anzenkanri_analysisreport.pdf.

[8] 中小企業庁, “2021年版　中小企業白書（HTML版）　第1部　令和2年度（2020年度）の中小企業の動向　第2章　中小企業・小規模事業者の実態　第1節　多様な中小企業・小規模事業者,” [オンライン]. Available: https://www.chusho.meti.go.jp/pamflet/hakusyo/2021/chusho/b1_2_1.html.

[9] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2020年度第4四半期,” 18 6 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_4q_securityreport.pdf.

[10] 個人情報保護委員会, “中小企業の皆様（中小企業サポートページ）,” [オンライン]. Available: https://www.ppc.go.jp/purpose/SMEs/.

[11] 尼崎市, “個人情報を含むUSBメモリーの紛失事案について,” 28 12 2022. [オンライン]. Available: https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html.

[12] 斎藤健二（ITmedia）, “三菱UFJ信託が情報銀行事業開始　Dprimeで「お金の代わりに個人情報を預かる」,” 1 7 2021. [オンライン]. Available: https://www.itmedia.co.jp/business/articles/2107/01/news126.html.

[13] Uber Technologies Inc., “Security update | Uber Newsroom,” 16 9 2022. [オンライン]. Available: https://www.uber.com/newsroom/security-update/.

[14] Microsoft Corporation, “Cyber Signals: Defending against cyber threats with the latest research, insights, and trends - Microsoft Security Blog,”

3 2 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/02/03/cyber-signals-defending-against-cyber-threats-with-the-latest-research-insights-and-trends/.

[15] IDG Communications, Inc., “Multi-factor authentication fatigue attacks are on the rise: How to defend against them | CSO Online,” 22 9 2022. [オンライン]. Available: https://www.csoonline.com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html.

[16] Built In Inc., “MFA Fatigue: What It Is and How to Avoid It | Built In,” 3 11 2022. [オンライン]. Available: https://builtin.com/cybersecurity/mfa-fatigue.

[17] Microsoft Corporation, “DEV-0537 criminal actor targeting organizations for data exfiltration and destruction - Microsoft Security Blog,” 22 3 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/.

[18] Cisco Systems, Inc., “Cisco Talos shares insights related to recent cyber attack on Cisco,” 10 10 2022. [オンライン]. Available: https://blog.talosintelligence.com/recent-cyber-attack/.

[19] CISA (Cybersecurity & Infrastructure Security Agency), “Implementing Number Matching in MFA Applications,” 10 2022. [オンライン]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf.

[20] Microsoft Corporation, “Use number matching in multifactor authentication (MFA) notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn,” 22 1 2023. [オンライン]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match.

[21] Microsoft Corporation, “Defend your users from MFA fatigue attacks - Microsoft Community Hub,” 28 9 2022. [オンライン]. Available: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677.

[22] CISA (Cybersecurity & Infrastructure Security Agency), “Implementing Phishing-Resistant MFA,” 10 2022. [オンライン]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[23] Research, Trend Micro, “Defending the Expanding Attack Surface: Trend Micro 2022 Midyear Cybersecurity Report,” 31 8 2022. [オンライン]. Available: https://documents.trendmicro.com/assets/rpt/rpt-defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report.pdf.

[24] AV-TEST, “AV-ATLAS - Malware & PUA,” 2022. [オンライン]. Available: https://portal.av-atlas.org/malware/statistics.

[25] Q-Success, “Usage Statistics and Market Share of Operating Systems for Websites, December 2022,” 16 12 2022. [オンライン]. Available: https://w3techs.com/technologies/overview/operating_system.

[26] Q-Success, “Usage Statistics and Market Share of Unix for Websites, December 2022,” 16 12 2022. [オンライン]. Available: https://w3techs.com/technologies/details/os-unix.

[27] ITmedia Inc., “日本企業の約4割がSaaS利用　ガートナー「クラウドは普及・拡大フェーズ」 - ITmedia NEWS,” 14 6 2021. [オンライン]. Available:

https://www.itmedia.co.jp/news/articles/2106/14/news132.html.

[28] IBM, “IBM Security X-Force脅威インテリジェンス・インデックス | IBM,” 2 2022. [オンライン]. Available: https://www.ibm.com/reports/threat-intelligence/jp-ja/.

[29] Intezer, “OrBit: New Undetected Linux Threat Uses Unique Hijack of Execution Flow,” 6 7 2022. [オンライン]. Available: https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/.

[30] Atlantic.Net, “OrBit Malware and Linux | What Is OrBit Malware? | Atlantic.Net,” 20 9 2022. [オンライン]. Available: https://www.atlantic.net/dedicated-server-hosting/orbit-malware-and-linux/.

[31] Red Hat, Inc., “2.3. /proc 仮想ファイルシステム Red Hat Enterprise Linux 7 | Red Hat Customer Portal,” 2022. [オンライン]. Available: https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/storage_administration_guide/proc-virt-fs.

[32] Linux man-pages project, “ld.so(8) - Linux manual page,” 18 12 2022. [オンライン]. Available: https://man7.org/linux/man-pages/man8/ld.so.8.html.

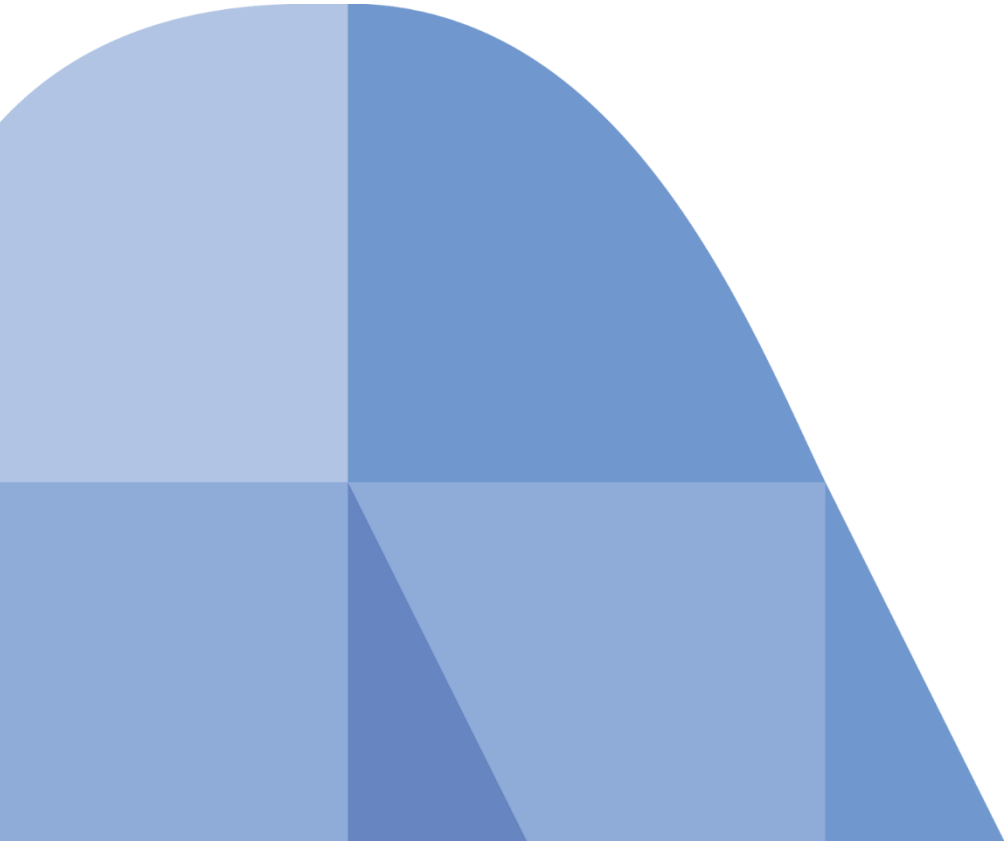
[33] AT&T Alien Labs, “Shikitega - New stealthy malware targeting Linux | AT&T Alien Labs,” 6 9 2022. [オンライン]. Available: https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux.

[34] Kaspersky, “What is an infection chain? | Kaspersky IT Encyclopedia,” [オンライン]. Available: https://encyclopedia.kaspersky.com/glossary/infection-chain/.

[35] Mandiant, “Shikata Ga Nai Encoder Still Going Strong | Mandiant,” 21 10 2019. [オンライン]. Available: https://www.mandiant.com/resources/blog/shikata-ga-nai-encoder-still-going-strong.

[36] Check Point Software Technologies LTD., “OPWNAI : Cybercriminals Starting to Use ChatGPT - Check Point Research,” 6 1 2023. [オンライン]. Available: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/.

[37] 医療法人社団鴻愛会　こうのす共生病院, 16 1 2023. [オンライン]. Available: https://kouaikai.jp/category/notice/.



Published on March 30, 2023

NTT DATA Corporation
Cyber Security Department
Hisamichi Ohtani
Toshihiko Matsuo / Yuki Wako / Kohei Takita / Teppei Sekine / Masayuki Matsubara
nttdata-cert@kits.nttdata.co.jp