NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

3rd Quarter of 2019

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary

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

OAuth for Office 365 targeted

Microsoft's Office 365 uses OAuth, the standard framework for authorizing access privileges, in order to cooperate with other services and applications. However, since vulnerabilities were found in the implementation of OAuth for Office 365, a phishing campaign aiming to hijack Office 365 accounts was conducted in the 3rd quarter of 2019. Although service cooperation using cooperation protocols such as OAuth or SAML is very convenient, damage is expected to be serious when it is exploited. Cloud service administrators of companies using the cloud should configure appropriate security setting. It is also recommended that administrators periodically check the list of applications that cooperate with the cloud service, attract ordinary users' attention, and perform compulsory administration for application cooperation.

Internal improprieties

In December 2019, an incident occurred where HDDs containing administrative documents of the Kanagawa Prefectural Government were sold via Internet auctions. It was due to internal improprieties by an employee of Broadlink Co. that was commissioned to discard hard disks. On the other hand, an incident was reported by the press where an employee of Trend Micro Incorporated illegally took out individual customer information and sold it on the black market, which was exploited for attacks. Both of the above are internal impropriety cases in companies specialized in security, and security measures were already taken. However, they are not enough as measures against internal improprieties and their operation was partially inappropriate. In order to prevent internal improprieties, it is necessary to formulate and introduce security measures assuming internal improprieties and analyzing their risks and ensure appropriate operation.

Attack on POS systems increasing in the US

Many incidents of credit card data breach due to attacks on POS systems have been reported

in the US. The US Government and international credit card brands are promoting migration from settlement by a magnetic stripe, which is vulnerable to attacks such as skimming, to the settlement standard using an IC chip called EMV. Industries that had not conducted this migration sufficiently enough were especially targeted. Make efforts in taking security measures recognizing that credit card information is always targeted by cybercriminals because it is directly connected with money.

Outlook

Cyberattacks are becoming increasingly sophisticated and diversified.

There are many cases where ransomware is used for intimidation backed by leaks of stolen information, and it is possible that industries and organizations more susceptible to intimidation will be targeted in future. Emotet was rampant in the 3rd quarter of 2019. It can be utilized to perform other attacks such as guiding users to a false site more effectively, using its ability to steal emails.

There is a possibility that attacks aiming to hijack accounts will increase accompanied with the prevalence of cloud services such as SaaS and IDaaS. Measures for restoration assuming accidents will be needed more in future.

2. Featured Topics

2.1. OAuth for Office 365 targeted

OAuth is a standard framework for authorizing access privileges to API or data for applications of 3rd parties. The latest version as of February 2020 is OAuth 2.0, and it was issued as RFC6749 [1] and RFC6750 [2]. Complying with this standard, the mechanism of API cooperation is implemented in various web applications such as Twitter and Facebook. Using this mechanism, users can make multiple applications and services cooperate together. Although it is a convenient mechanism, attackers launch attacks trying to exploit this. In 2012, IPA was sending notices about a case where an account was hacked due to service cooperation using unintended OAuth [3]. In this 3rd quarter of 2019, a characteristic attack was discovered that hacked an Office 365 account exploiting the OAuth mechanism. Office 365 is a SaaS service Microsoft is working with and provides not only office applications and email services but also the ID cooperation services and the internal chat service "Teams" for corporate customers [4]. If Office 365 accounts of corporate customers are hijacked, it is assumed that classified information inside companies may be stolen or may be exploited as the sender of spam email or targeted attack emails. Table 1 shows the list of events related with OAuth occurred in the 3rd quarter of 2019.

Table 1: Events related with OAuth

No.	Date	Summary
1	12/2	CyberArk published the vulnerability "BlackDirect" where accounts of Office 365 or Azure can be hijacked by exploiting the mechanism of OAuth. [5] [6]
2	12/9	PhishLabs published a phishing campaign where the attacker tries to steal an OAuth token to exploit in a malicious Office 365 application instead of the Office 365 user ID and password [7].

2.1.1. Vulnerability “BlackDirect”

The attacker leads the victim in a log-in state to Office 365 to access the link provided by the attacker and acquires an OAuth token exploiting the vulnerability of No. 1 in Table 1.According to CyberArk’s explanation, the causes of the vulnerability are as follows:

1. The mechanism implemented in the Office 365 application is such that the OAuth token requested by each application is transferred to the redirect URL specified in the “ReplyUrls” parameter.
2. Microsoft had registered the URL of the redirect destination to the whitelist in some applications. Token transfer to the URLs registered on the whitelist is automatically executed.
3. A subdomain in a domain registered on the whitelist could be acquired by anyone via a Microsoft service.

When the attacker requested the OAuth token for an application he/she had created after acquiring the subdomain, he/she could automatically acquire the token as Microsoft applications could by specifying the URL of the acquired subdomain. The attacker who has acquired the token can perform all Office 365 operations with the same privilege as the user who has issued the token.
CyberArk published the demonstration video of this attack [8]. In this video, the victim accesses a suspicious link in a log-in state to Office 365, so the attacker’s application is associated with the Office 365 account and steals the issued OAuth token and a user account is created for the attacker.
This vulnerability was reported to Microsoft on October 20 and fixed on November 19.

2.1.2. OAuth phishing campaign

The phishing campaign of No. 2 in Table 1 uses the method of making an Office 365 application cooperate with an account and guiding it to an URL that requests issue of an OAuth token to steal the OAuth token, which is the same as No. 1, instead of guiding an Office 365 user to a false site and stealing the ID and password like existing phishing emails.

The method used by existing phishing emails is as shown in Figure 1.

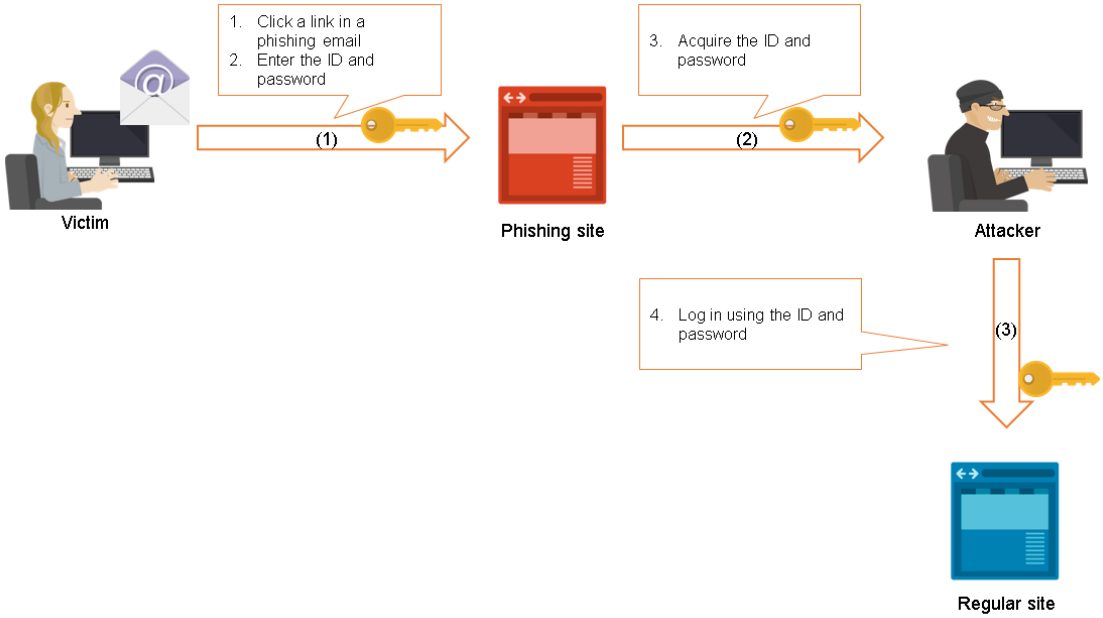


Figure 1: Method used by ordinary phishing emails

1. The user of an authorized site clicks a link in an email the attacker sent and is guided to a phishing site that imitates the authorized site.
2. The user inputs his/her ID and password for the authorized site to the phishing site.
3. The attacker acquires the user's ID and password for the authorized site from the phishing site.
4. The attacker logs in to the authorized site using the acquired ID and password.

For this existing method of phishing email, stealing IDs and passwords can be prevented if the user can check whether the linked domain is an authorized site or an imitated site. In addition, even if the ID and password are stolen, unauthorized log-in can be prevented if the authorized site uses two-factor authentication as the log-in authentication method.

The new method discovered this time guides the user to an authorized Microsoft site, so the decision cannot be made based on whether the domain is authorized or not like phishing emails. In addition, since an OAuth token is acquired, unauthorized access cannot be prevented even if Office 365's two-factor authentication is enabled. It cannot be prevented even if the password is changed.

The method used by the new phishing emails is as shown below:

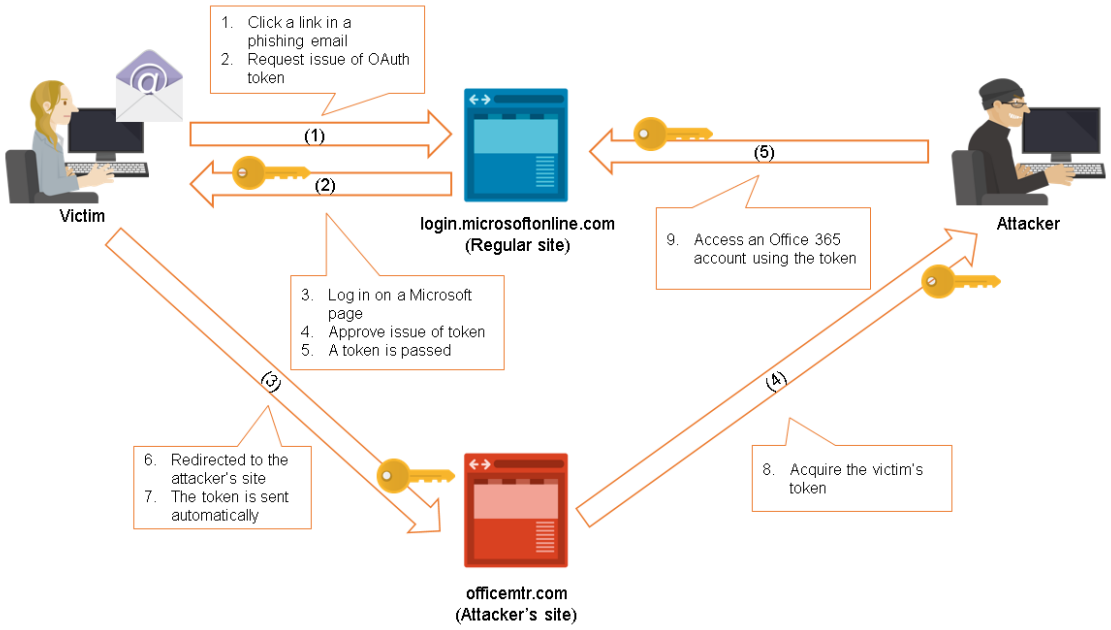


Figure 2: Method used by new phishing email

1. An Office 365 user clicks a URL link in an email the attacker sent and is guided to "login.microsoftonline.com".
2. At the same time as 1, issue of an OAuth token to be given to an Office 365 application provided by the attacker is requested by a parameter specified in the URL link.
3. The user logs in to "login.microsoftonline.com".
4. The user approves the issue of an OAuth token.
5. The OAuth token is issued and sent to the user.
6. Since the attacker sets a redirect, the OAuth token is transferred to the attacker's site "officemtr.com" after it is sent to the user.
7. The OAuth token is automatically sent to the attacker's site "officemtr.com".
8. The attacker acquires the OAuth token from the site "officemtr.com".
9. The attacker accesses the user account of Office 365 using the acquired OAuth token.

The attacker is using multiple techniques in order to succeed using this attack method.

Technique 1 “phishing email text” (Step 1 of Figure 2)

The attacker creates and sends a phishing email without suspicious contents to lead an Office 365 user to log in to an Office 365 site.

- Example of phishing email contents:
  - Notification of OneDrive Excel file sharing (refer to Figure 3)
  - Notification of Office 365 account password expiration (refer to Figure 4)

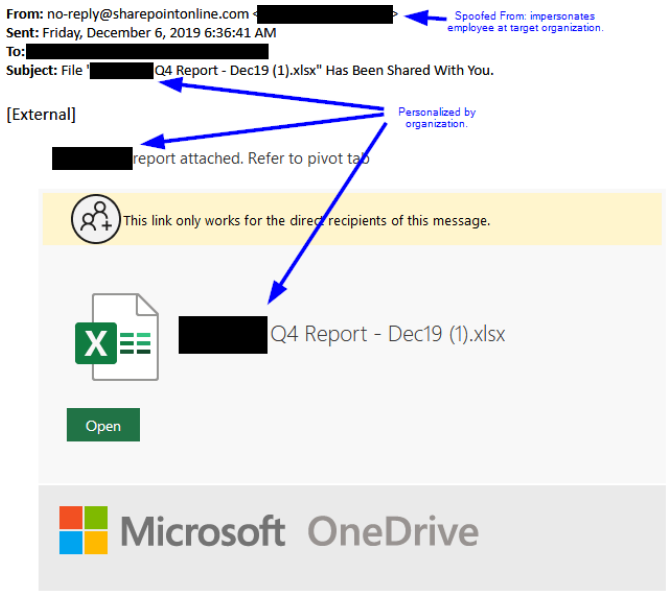


Figure 3: Phishing email notifying OneDrive Excel file sharing (reproduction of [7] in The PhishLabs Blog)

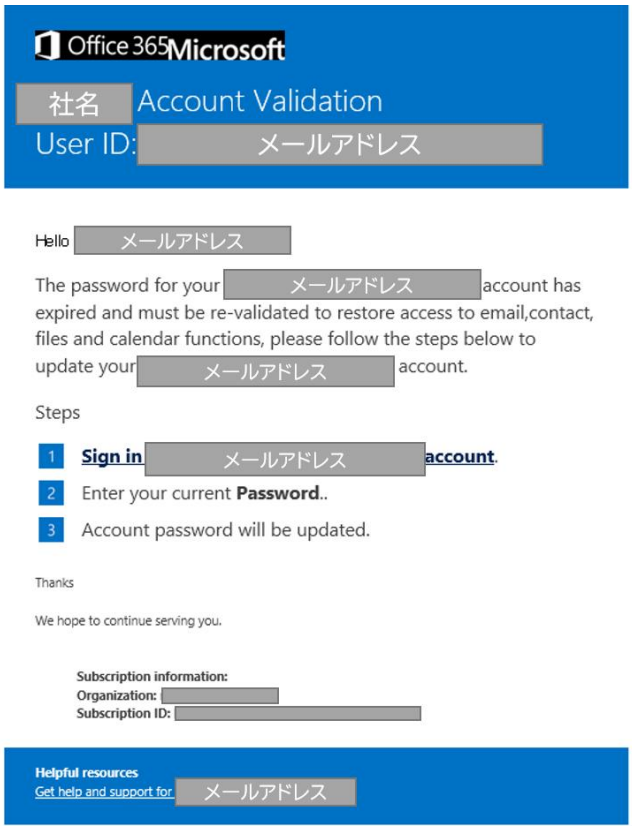


Figure 4: Notification of Office 365 account password expiration

Technique 2 “URL link” (Step 2 of Figure 2)

The URL of Figure 2 is shown in the URL link in the phishing email. In this URL, a URL parameter is set that issues an OAuth token for the attacker’s application and transfers it to the attacker’s site. Since the domain and the URL parameter are in the proper format complying with the rules of the Microsoft Office 365 site, it is difficult to notice any suspiciousness based on the URL link.

Figure 2: URL pattern in phishing email

URL pattern
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?%20client_id={client_id} &response_type=id_token+code&redirect_uri={Redirect_uri} &scope={authority to request} &state={state}&response_mode=%20form_post&nonce={nonce}

Technique 3 “Authorized approval page” (Step 4 of Figure 2)

In Step 4, the screen in Figure5 is displayed and the user is requested to approve issue of an OAuth token for an application. In the issue of an OAuth token, the authorities the attacker wants to acquire in advance are specified. If the user approves the issue of the OAuth token, the application can acquire those authorities the attacker specified. In the example in Figure5, approval for persistent access and read-out authority of the profile is given to the application. Given the authority, the attacker conducts various fraudulent actions using the application.

Figure5: Example of authority request

NTTDATA-CERT performed a verification experiment constructing a sample application for attack verification and a simulation site that is equivalent to the attacker’s site in Figure 2.As the result, OneDrive and Teams, which can be accessed only from the internal network, were able to be accessed from anywhere on the Internet when the sample application for attack verification was used.

2.1.3. Attack detection, temporary measures, and proactive measures

Both No.1 and No.2 of Table 1 are attacks exploiting the OAuth token issue process accompanied with Office 365 application cooperation. These attacks can be detected investigating the status of application cooperation.

Attack detection method

As shown in Figure 6, the administrators of Office 365 and Azure acquire the list of enterprise applications currently cooperating with tenants using the Azure portal and check if there is any suspicious application. If there is an application with an unfamiliar name, there is a possibility that an attack has succeeded.

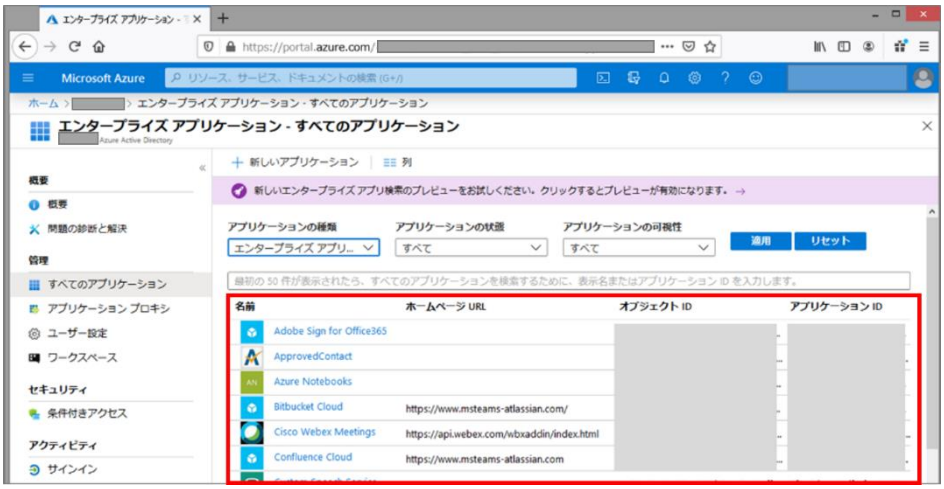


Figure 6: Check of application registration status in Azure portal

Temporary measures

If there is a suspicious application, its sign-in can be disabled by changing the indicated part to “No” in its properties screen shown in Figure 7.

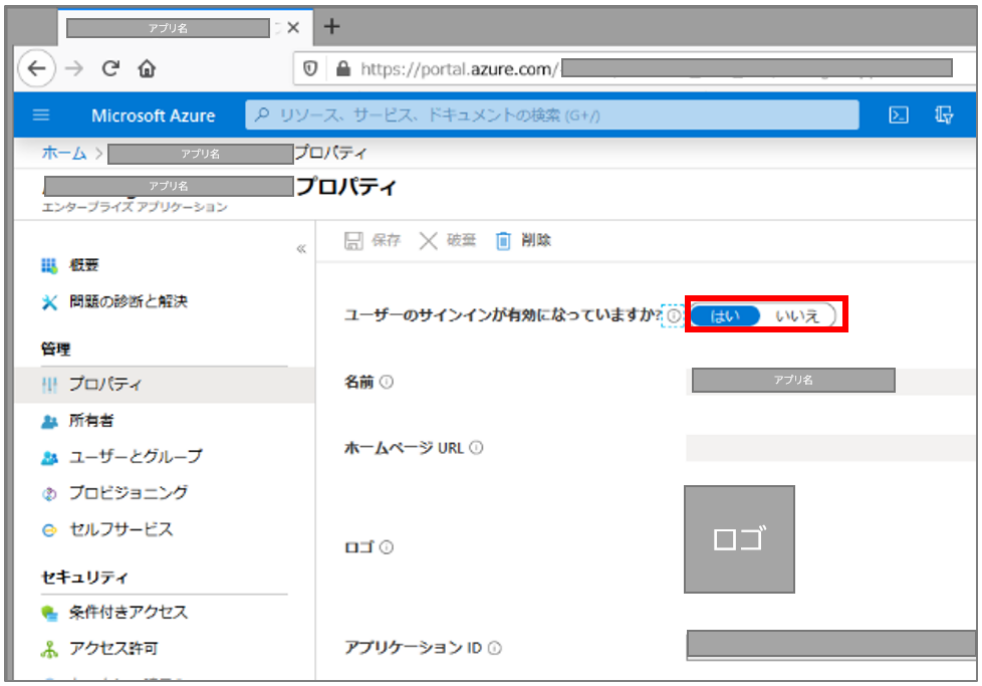


Figure 7: Disabling application in Azure portal

Proactive measures

If the administrators of Office 365 and Azure perform setting to restrict issue of OAuth for applications of general users in the Azure portal, issue of OAuth token for suspicious applications can be prevented. General users cannot approve issue of OAuth token for applications if the corresponding item of Azure active directory settings is set to “No” as shown in Figure 8.

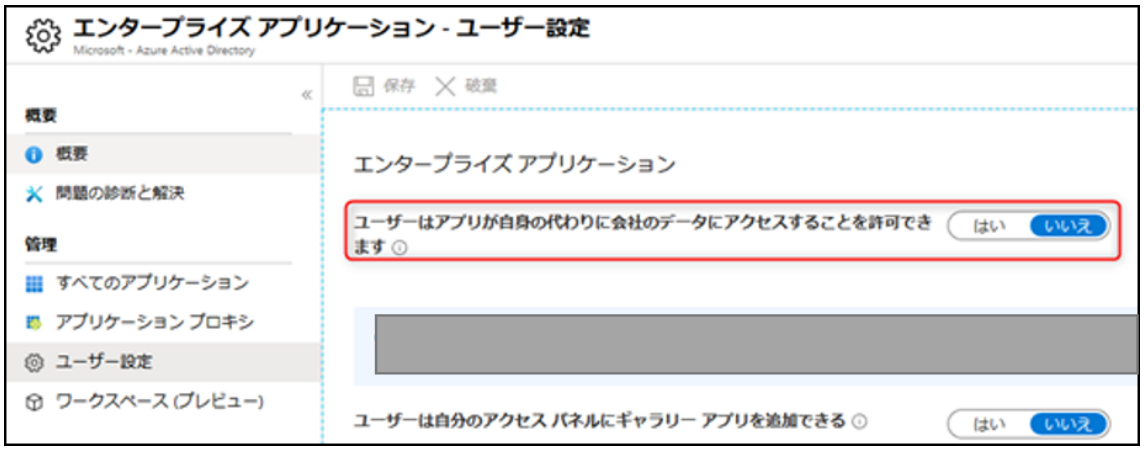


Figure 8: Prohibiting general user’s approval for application cooperation

2.1.4. Conclusion

Whereas convenience for users is improved in association with the increased number of cloud services supporting application cooperation protocols such as OAuth and SAML, an increase in the number of attacks that steal tokens for cooperation is predicted. Since it is difficult to detect an exploit of these tokens, damage that occurs when tokens are stolen is expected to become more serious accompanied with the increasing use of cloud services. Administrators of cloud services of companies using the cloud should perform appropriate security setting. It is also recommended that administrators periodically check applications that cooperate with the cloud service, attract ordinary users' attention, and perform compulsory administration for application cooperation.

2.2. Internal improprieties

Damage per information security incident due to internal improprieties is often larger than that caused by an attack from outside, and it sometimes has a significant impact on business once it has occurred.

In the 3rd quarter of 2019, an incident occurred where used hard disks (HDDs) of the Kanagawa Prefectural Government containing a large amount of personal information and confidential information were sold and leaked via Internet auctions. In this incident, an employee of Broadlink Co., which is a company specialized in security, sold the HDDs, for which he was commissioned to perform data erasure and physical destruction, via Internet auctions without conducting destruction [9]. The number of HDDs and other recording mediums this employee sold is more than 3,500 and it is unknown how many of them were the ones he stole from Broadlink Co. On top of that, Broadlink Co. was commissioned to discard hard disks by various government and municipal offices as well as the Kanagawa Prefectural Government and there is concern that the scope of impact will expand. [10] As a consequence, the company paid a huge price, firing 10% of employees and closing more than one office while the president expressed his intention of retirement [11].

Similarly, there was a leak of personal information due to internal improprieties at Trend Micro Incorporated, which is a company specialized in security. This case was related with overseas user support where information about individual users was taken out due to fraudulent actions by a former employee and received by a third party who exploited it for crime. The information that was taken out is related with support for English-speaking users of security products sold overseas to individuals. [12]

In the following sections, we consider why internal improprieties occurred in those two companies specialized in security and what measures against internal improprieties should be taken by using the Broadlink case as an example.

2.2.1. Difficulty in implementing measures

Donald Ray Cressey, a researcher of organized crime in the US, advocated a theory called “fraud triangle” that says internal improprieties occur when three elements of “perceived pressure”, “perceived opportunity” and “rationalization” are all present [13]. This is the idea that internal improprieties can be reduced by reducing opportunities for conducting them or reducing profit obtained from them to suppress motives so that not all of these three elements are present.

That company had been taking the measures shown in Table 3 [14]. However, they are mainly measures against intrusion of a suspicious person, theft, and careless mistakes and there are only two measures that can eliminate internal improprieties.

Table3: Existing measures of Broadlink against internal improprieties

No.	Measure	Summary	Effect against internal improprieties[1]	
1	Entering and leaving using card keys and fingerprint authentication	Area for arrival of goods: Entering and leaving using card keys Data erasure: Entering and leaving using card keys and fingerprint authentication Area for packing and shipment: Entering and leaving using card keys	—	This is a measure against suspicious persons and unauthorized persons and no effect is expected against internal improprieties with authorization for entering and leaving.
2	Entering and leaving log management	Employee unique ID keys, door numbers, entering times, and leaving times are recorded to show who entered and left and when.	△	Although a deterrent effect can be expected by auditing the entering and leaving logs and detecting suspicious times, improprieties can be conducted.
3	24-hour surveillance camera	24 hours recording by surveillance camera	△	Although a deterrent effect can be expected by recording fraudulent actions, fraudulent actions cannot be prevented.
4	Individual management for each device	Manage individual packs from arrival of each device until data erasure and shipment by attaching a control number and a control bar code label to each individual device.	○	Deterrent effect is high because internal improprieties can be detected early if total number management is always conducted.
5	Personal belongings management (bringing-in prevention)	Install exclusive-use lockers to prevent bringing-in of personal belongings to facilities.	—	This is a measure against bringing-in of PCs and mobile phones and no effect is expected against bringing-out of HDDs.

[1] "internal fraud" in this table is evaluated focusing on the effect on bringing-out of HDDs. Internal fraud not related to bringing-out of HDDs is indicated as "-".

6	Personal belongings management (bringing-out prevention)	Conduct baggage inspection for bringing-out prevention	○	"Opportunities" can be eliminated because bringing-out of HDDs can be discovered and prevented.
7	Opening/closing alarm	Alarm starts if opened for 1 minute.	—	This is a measure against suspicious persons and unauthorized persons and no effect is expected against internal improprieties with authorization for entering and leaving.
8	Exclusive-use uniform with sewn pocket	Exclusive-use uniforms are worn on which pockets are sewn.	—	This is a measure against careless bringing-out of USB memories.

Legend: ○: effective measures against bringing-out of HDDs
△: only a limited deterrent effect
－: not effective measures against bringing-out of HDDs

Measures whose effect is "△" like "24-hour surveillance camera" shown as No. 3, in Table 3 have only a deterrent effect and cannot prevent fraudulent actions by authorized but malicious internal persons. 2 items, No. 4 and No. 6, in Table3 are measures whose effect against internal improprieties can be expected. However, these measures were not operated appropriately as shown in Table4.

Table4: Operation status of measures whose effect against internal improprieties in Table3 can be expected

No.	Measure	Summary	Reason for no effect against internal improprieties
4	Individual management for each device	Manage individual packs from arrival of each device until data erasure and shipment by attaching a control number and a control bar code label to each individual device.	If individual management until shipment had been performed appropriately, fraudulent bringing-out of HDDs would have been detected immediately. Since it was not noticed until pointed out by outside persons, it can be assumed that operation was not performed appropriately.
6	Personal belongings management (bringing-out prevention)	Conduct baggage inspection for bringing-out prevention	It has been reported that baggage inspection was "conducted on an irregular basis and not frequently enough".

Since the employee who committed the internal improprieties said it was easy if going there before the working hours according to media reports, we can see he conducted bringing-out of HDDs after finding the measures against internal improprieties were not sufficient [15]. It can be assumed that the measures in Table3 are not security measures created based on risk analysis assuming internal improprieties but ones created gathering best practices for data breach measures. It seems to be the reason why effects sufficient for preventing internal improprieties did not occur. In addition, even if measures against internal improprieties are created and introduced, internal improprieties are not prevented if appropriate operation is not performed.

2.2.2. Idea of measures against internal improprieties

Broadlink Co. announced that it will implement the following additional measures [14]. However, when we see the additional measures in Table5, similarly to the existing measures of Broadlink in Table3 against internal improprieties, we found there are measures that are not expected to be effective against malicious persons who commit internal improprieties.

Table5: Additional measures of Broadlink against internal improprieties

No.	Measure	Reason for no effect against internal improprieties[2]	
1	Make photographing of all HDDs before and after physical destruction mandatory	△	If photographing of HDDs before and after destruction is performed so that the unique number of the HDD can be seen, the identity of the HDD can be proved. It is also needed to check there are photographs of all HDDs.
2	Manned body check using a handy metal detector and baggage inspection conducted at entering and leaving during the operation time zone	○	It will be effective if a room dedicated to erasure and physical destruction of HDDs is established and prohibition of entering and leaving outside the operation time zone and the measures shown on the left are performed. However, there is a possibility that bringing-out is conducted outside the operation time zone.
3	Establish entering and leaving security gates and conduct body check using a handy metal detector and baggage inspection by a security guard	△	Measures against fraudulent bringing-out of HDDs received from customers before bringing-in to the dedicated room. Bringing-out is possible if not checked in 24 hours.
4	Additional security cameras	△	Although the deterrent effect is improved, fraudulent actions cannot be prevented completely. Work for checking video is also necessary.
5	Periodic security training by an outside lecturer	—	There is no effect against internal improprieties with a strong malicious intention or a criminal intention.

Legend: ○: effective measures against bringing-out of HDDs
△: only a limited deterrent effect
—: not effective measures against bringing-out of HDDs

The additional measures in Table5 are assumed to be created by partially strengthening Broadlink's existing measures against internal improprieties in Table3.They do not seem to be security measures created based on risk analysis mainly on internal improprieties concerning the work of data erasure and physical destruction of HDDs in Broadlink.

Although the above description referred to measures against internal improprieties using the

[2] "internal fraud" in this table is evaluated focusing on the effect on bringing-out of HDDs. Internal fraud not related to bringing-out of HDDs is indicated as "-".

fraud triangle, since Ronald Clarke's situational crime prevention theory and rational choice theory described below are easier to derive measures against internal improprieties, the following description recommends measures derived using only measures that prevent internal improprieties in the field of information security [16].

- Situational crime prevention
  Focusing on spatial aspects of crime (crime opportunity/situation), prevent crimes by decreasing crime opportunities.
- Rational choice theory
  Humans choose their behavior rationally calculating profit and loss.
  ① Raise the difficulty level of crime (Example: Make intrusion harder)
  Introduce measures to prevent or directly thwart certain actions of internal improprieties
  ② Raise the risk of detection of crime (Example: Secure surveillance)
  Enhance control and surveillance to detect internal improprieties, introduce measures to identify persons who commit internal improprieties
  ③ Decrease earned reward (Example: Remove objects of crime)
  Do not handle expensive assets, lower asset value

In other words, if disadvantage from detection of internal improprieties and certain demerits of committing internal improprieties become greater than profit from internal improprieties, internal improprieties can be prevented because of reduced motives.

Table6: Recommended measures based on rational choice theory

	Principle	Summary
①	Raise the difficulty level of crime	Stop fraudulent bringing-out of HDDs. Introduce a procedure where HDDs entrusted by a customer are locked, conveyed, and taken out only in the room dedicated to work. Lock the entrance door and prohibit entering and leaving outside the operation time zone. Bringing-out of destroyed HDDs is allowed. The number of destroyed HDDs should be confirmed and reported by 2 or more persons.

②	Raise the risk of detection of crime	Conduct recording by surveillance cameras and check of video. Prohibit in principle bringing-in/bringing-out of goods to the room dedicated to work and conduct body check at entering and leaving.
③	Decrease earned reward	Physical destruction is performed for all HDDs that cannot be sold.

2.2.3. Conclusion

In the case of this time, security measures such as entering and leaving management and surveillance had been conducted but they were insufficient as measures against internal improprieties. Furthermore, with the inappropriate operation where baggage inspection was conducted on an irregular basis, the affair developed into the situation where a leak of a huge amount of personal information and confidential information occurred.

In order to prevent internal improprieties, what is necessary is not to gather best practices for data breach measures and perform them but to formulate and introduce security measures assuming internal improprieties and analyzing their risks and ensure appropriate operation.

In order to prevent internal improprieties, companies are expected to make disadvantages from detection of internal improprieties and certain demerits of committing internal improprieties become greater than profit from internal improprieties and reduce motives for committing internal improprieties.

For companies specialized in security and other organizations that have to put importance on security, it is necessary not only to reduce motives for committing internal improprieties but also to consider measures such as encryption of information in order to reduce damage as much as possible in the case of leakage assuming occurrence of internal improprieties.

3. Data Breach

3.1.1. POS Attacks Growing in the US

In the 1st quarter and the 2nd quarter of 2019, the increase of attacks that steal credit card information from EC sites by Web skimming was published. In the 3rd quarter of 2019, whereas Web skimming has been still being detected, many incidents of credit card data breach due to attacks on POS systems at physical stores have been reported in the US.

In all the cases shown in Table7, infection with malware called POS malware, which is a POS-specific malware, occurred and credit card information was stolen by POS malware when the credit card information was read from the magnetic stripe at settlement. The POS malware automatically collects credit card information such as card number, name, and expiration date and sends it to the outside attacker. A criminal receives the credit card information from the attacker and performs fraudulent use by spoofing.

Table7: Cases of data breach incident with POS malware

Date	Target		Summary
10/3	Hy-Vee	Retailing (supermarket, gas station)	Report on investigation result about case of infection with POS malware in part of payment processing system [17]. 5.3 million pieces of card information that had been stolen were sold on the dark web. [18] Compromise period: December 2018 - August 2019
10/24	Krystal	Food service industry (fast food)	Part of payment processing system was infected with POS malware [19]. 4 million pieces of card information that had been stolen were sold on the dark web. (including card information stolen at Focus Brands in August, 2019) [18]) Compromise period: July 2019 - September 2019
11/13	Gas station	Fuel retailing	Visa reported 2 cases of attack with POS malware that occurred at a gas station in North America [20].
12/11	Gas station	Fuel retailing	Visa reported 3 cases of attack with POS malware that occurred at a gas station in North America [21].

12/20	Wawa	Retailing (convenience store, gas station)	Payment processing system was infected with POS malware. More than 850 business bases are impacted [22]. Compromise period: March 3, 2019 - December 10, 2019

3.1.2. Flow of attack on POS systems

Attacks on POS systems are performed as shown in the following flow:

1. The attacker intrudes into the network of the target company. The means for intrusion is targeted attack and exploiting of server vulnerability published on the Internet or setting defects.
2. The attacker acquires the authentication information of the POS system by spying on the network of the target company and intrudes into the POS system operated by the company. After intruding into the POS system, the attacker infects settlement terminals at each store with POS malware called RAM scraper.
3. At the settlement process, the credit card information read by the magnetic reader is stored in the memory as plain text. RAM scraper searches the memory, picks out the card information, and sends it to the outside illicitly.

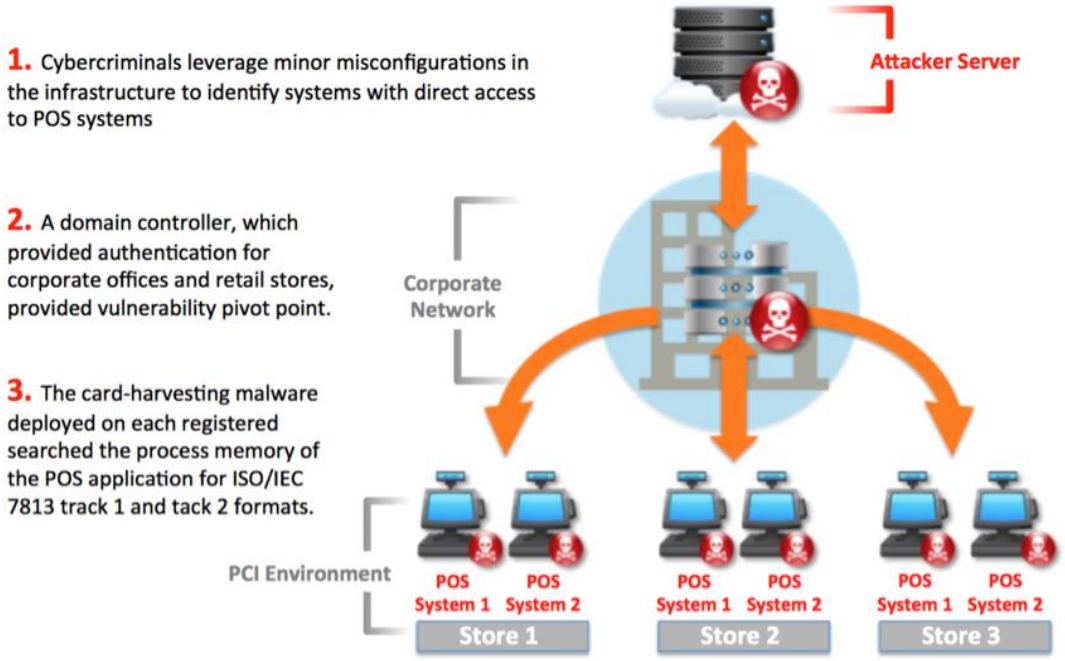


Figure9: Attack model using POS malware
(cited from VMware Carbon Black Security Blog) [23]

3.1.3. Security measure trend in the US

Since magnetic stripes are vulnerable in security, migration to IC chips is being performed globally. The international unified standard of credit card with IC chips is called EMV, and the settlement process using IC chips can be realized if both credit cards and settlement terminals comply with EMV. As a measure against POS malware described above, it is said that discontinuation of using plain-text credit card information in the POS system in addition to compliance of credit card and settlement terminals with EMV is effective. [24]

In the US, many companies such as Home Depot, Hyatt, and Target were damaged by credit card data breaches in 2013. Especially, in the case of Target, it is said that 40 million pieces of credit card information were leaked. [25] In response to this, the Federal Government issued a presidential decree about security of credit card settlement in 2014 to make it obligatory to issue credit cards complying with EMV. Furthermore, international credit card brands started operation with liability shift in 2015 in order to promote introduction of settlement terminals complying with EMV. Liability shift is the rule where member stores, not credit-card issuing companies, are liable to obligation if the settlement process is performed with a forged credit card at a terminal non-compliant with EMV. Since installation of new terminals requires time and money, the due date for responding to liability shift (installation of settlement terminals complying with EMV and accompanying modification of system) is set to October 2017 in principle. Furthermore, for gas stations, since special technologies for refueling and complex infrastructure are used, the due date for responding to liability shift is set to October 2020.

According to a blog article by Kaspersky Lab at that time, damage at retailing stores due to credit card data breach increased in 2016, which was the migration period for responding to liability shift. It is assumed that attackers were actively attacking terminals not-complying with EMV before October 2017, the due date for responding to liability shift [26].

In the reminder sent by Visa in November and December 2019, an increase in the number of attacks targeting gas stations and the possibility of the involvement of the cybercriminal group “FIN8” were pointed out [20] [21]. FIN8 is a high-level cybercriminal group that steals credit card information using POS malware. Although it was active in 2016 and 2017, their activity was declining after 2017. However, it is now active targeting gas stations. With less than one year left until the due date for responding to liability shift, there is a possibility that FIN8 has started activity again and is conducting last-minute attacks targeting settlement terminals with a magnetic stripe as was the case with 2016. Caution against POS malware is still required.

3.1.4. Conclusion

This chapter featured the trend in which theft of card information from long-existing POS systems is increasing whereas theft of card information by Web skimming is becoming mainstream. In Japan, there are requirements to cards/settlement terminals at counter-type member stores such as supporting IC and discontinuation of holding card information by March 2020 according to the Installment Sales Act, which came into force in June 2018. However, according to a survey conducted by The Japan Consumer Credit Association in July 2019, 61.8% of credit cards are supporting IC. Magnetic stripes is still in use [27]. As long as the use of magnetic stripes continues, there is a possibility that POS malware attacks will concentrate in Japan.It is important for organizations handling credit cards to conduct security measures described above promptly and prevent data breach in advance considering that the number of crimes tends to increase before and after due dates for responding to policies and legislation as shown in the cases in the US. Furthermore, to quickly find occurrence of unauthorized use, users of credit cards should periodically check whether there are transactions in their credit card statements of which he/she has no recollection.

If it becomes difficult to steal credit card information from POS systems in the future due to enhancement of security measures, there are concerns that the number of victims due to other methods such as Web skimming at EC sites and guiding to phishing sites using emails will increase. Make efforts in taking security measures recognizing that credit card information is always targeted by cybercriminals because it is directly connected with money.

4. Vulnerability

4.1. Vulnerability of PHP-FPM

Vulnerability discovered at “Capture the Flag”

The PHP Group published information about CVE-2019-11043, vulnerability of PHP-FPM. This vulnerability is vulnerability of PHP-FPM (FastCGI Process Manager), which is one of the implementations of FastCGI of PHP. In the case of certain configuration and certain settings, any code can be executed remotely.

The impacted systems are limited because conditions such as certain version of PHP, certain configuration, and certain settings must be satisfied to exploit the vulnerability. However, since servers that satisfy the conditions generally exist, the vulnerability is dangerous. [28]

This vulnerability was first discovered at a security contest called CTF (Capture the Flag). [29] The flow of discovering vulnerability, publishing information, publishing PoC, and releasing a patch is as follows. This vulnerability was a zero-day vulnerability, which means no fixed version existed right after the information was published.

- 9/14 - 9/16: Mr. Andrew Danau, a researcher, discovered the bug at “Real World CTF 2019 Quals”.
- 9/26: Mr. Emil Lerner, a researcher, submitted the vulnerability information to “PHP Bug Tracking System”.
- 10/22: PoC was published on Github.
- 10/24: The PHP group released a fixed patch.

Attack on Web system combining nginx and PHP-FPM

It was found that the vulnerability of PHP-FPM can be exploited especially on a Web system constructed combining nginx and PHP-FPM. [30] The attacker can change the environment variables of PHP execution environment by exploiting a defect of linefeed code on the nginx side and the vulnerability of PHP-FPM. As a result of changing the environment variables, the attacker can execute any code remotely. According to a verification report by NTT Data Intellilink, the environment variables can be changed when the settings of nginx satisfy the following 4 conditions: [31]

1. In the settings of location directive, requests are to be transferred to PHP-FPM.
2. When assigning the PATH_INFO variables, the fastcgi_param directive is used.
3. The fastcgi_split_path_info directive exists and the regular expression, which begins with

"^" and ends with "$", is used.

4. There is no checking of file existence such as "try_files $uri =404".

nginx with settings that satisfy the 4 conditions generally exists. An example of setting file (.conf) that satisfies the above 4 conditions is shown below:

```
location ~ [^/]¥.php(/|$) {
    fastcgi_split_path_info ^(.+?¥.php)(/.*)$;
    fastcgi_param PATH_INFO $fastcgi_path_info;
    fastcgi_pass php:9000;
    ...
}
```

Exploiting of vulnerability by ransomware "NextCry"

Ransomware "NextCry" is observed. It targets "NextCloud", open source software that can construct an online storage, and tries to encrypt files. [32] Exploiting vulnerability of PHP-FPM, ransomware "NextCry" is infected with a Web system.

Nextcloud needs to be constructed preparing a Web server engine separately. Nginx is contained in one of the Web server engines. Nextcloud is now being targeted because it once recommended configurations using nginx in the past and possibility of succeeding in an attack is high. After publishing the vulnerability, Nextcloud sent a reminder to system administrators who use nginx. [33]

Exploiting vulnerability of PHP-FPM, NextCry performs the following actions. First, referring to the setting file of NextCloud "config.php", NextCry acquires the directory path used for storing data. Next, NextCry encrypts data stored at the acquired directory path and displays a threatening message on the administration screens and operation screens. Since the PoC was published before the vulnerability was published, it is assumed that NextCry exploited the vulnerability a few days after it was published.

Conclusion

It is difficult to handle zero-day vulnerabilities like PHP-FPM ones because there is a possibility that attacks occur before a formal fixed version is provided. When information about zero-day vulnerabilities is confirmed, damage by attacks should be minimized by taking actions such as implementing a workaround by changing the settings or monitoring suspicious communication. Furthermore, after updating to a fixed version, since there is a possibility of being attacked already, it is necessary to check if a falsification, suspicious

communication, or execution of illicit process has occurred.
The impact of vulnerability is large because PHP is a widely used script language. The vulnerability of PHP-FPM greatly impacted on nginx and Nextcloud. In some cases, there is impact from vulnerability of programing languages or libraries and not from vulnerability of the hardware or software product in use itself. Conduct appropriate vulnerability management grasping the characteristics of products you are using. If impact on products being used is suspected concerning vulnerability, it is useful to check with the product vendors about the impact.

4.2. Exploited vulnerabilities

Separately from vulnerabilities of PHP-FPM, a part of the vulnerabilities that were exploited or of which an exploiting attempt was confirmed in the 3rd quarter of 2019 are shown in Table8.

Table8: Vulnerabilities for which exploiting was confirmed

Vulnerability No.	Target	Summary
CVE-2018-0296	Cisco ASA	Rapid increase of attacks exploiting vulnerabilities is observed, and Cisco Systems changed the rating of importance level. [34]
CVE-2019-2215	Android	Privilege escalation vulnerability that impacts on Android 8.x and later. Pixel, Samsung, and Xiaomi are impacted. [35]
CVE-2018-7600 Drupalgeddon2	Drupal	A researcher of Akamai discovered a new campaign that distributes malware by exploiting the vulnerability. [36]
CVE-2019-11510 CVE-2019-11539 CVE-2018-13379	SSL VPN product	Vulnerability that drew attention because attacks exploiting it increased in September. [37] Multiple agencies including NSA issued a warning about exploiting by an attacker group. [38]
CVE-2019-18187	Virus buster	Vulnerability of directory traversal. TrendMicro confirmed an exploiting attack. [39]
CVE-2019-13720 CVE-2019-13721	Google Chrome	Vulnerability of memory use after releasing audio. There was a period of zero day, and an attack was also confirmed. [40]
CVE-2019-0708 BlueKeep	Windows RDP	Vulnerability found in May. Reminders were sent several times. CERT NZ sent a reminder again. [41]
CVE-2015-2419 CVE-2018-4878 CVE-2018-15982 CVE-2018-8174	Internet Explorer Adobe Flash Player	A researcher of TrendMicro confirmed that a newly discovered exploiting kit “Capesand” was exploiting the vulnerability. The report said it was continuously used for attacking as of October. [42]
CVE-2019-8144	Magento	Reminders were sent to users of Magento Commerce 2.3.x in order to prevent damage from attacks exploiting the vulnerability. [43]
CVE-2019-1429	Internet Explorer	Vulnerability of breakage of script engine memory. Zero-day attack was confirmed. [44]
CVE-2019-1458	Windows	Exploiting was performed by the campaign called “Operation WizardOpiu”. This was a zero-day vulnerability. [45]

5. Malware/Ransomware

5.1.1. Frequent occurrence of Emotet damage in Japan

Emotet is the malware that drew the most attention in the 3rd quarter of 2019. Refer to the report of the 1st quarter of 2019 for what malware Emotet is. [46] Quarterly Report on Global Security Trends featured Emotet in the 1st and 2nd quarter of 2019, but both are about cases overseas. However, a large-scale infection in Japan was confirmed in the 3rd quarter. Although the number of detected PCs in September was 86, it increased rapidly to 1700 in October and 8019 in December. [47] In December, JPCERT/CC and IPA sent a reminder [48] [49] and the situation developed into a press conference by the Chief Cabinet Secretary. [49] Why did the infection spread so widely in Japan?

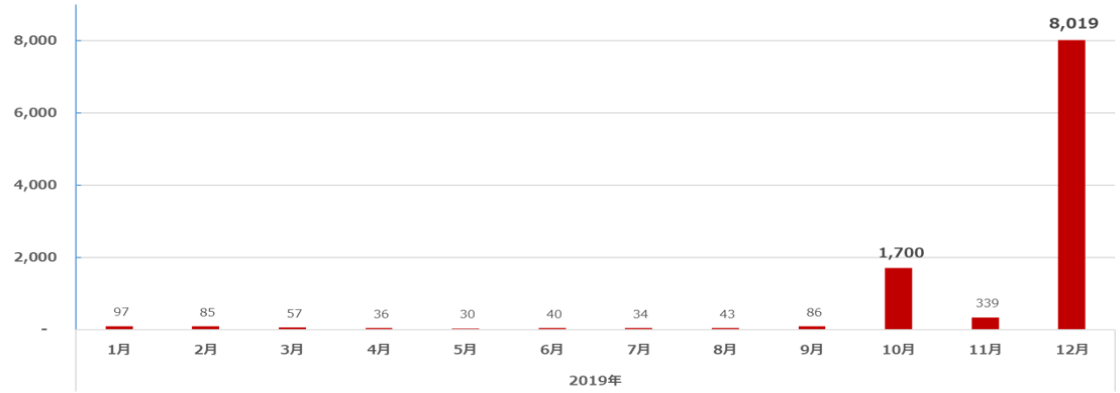


Figure 1: Transition of number of detected PCs in Japan
(cited from Trend Micro Security Blog)

The following 2 reasons can be given: The 1st reason is that it has become difficult to distinguish between normal and illicit Emotet emails sent from the attacker. In the text of an email, sentences that include irrelevant subjects or predicates are very few. Since the text has only about 3 lines of succinct Japanese with a high abstraction level (e.g. "Sanko made ni", "Gokakunin onegai shimasu"), the succinct Japanese seems to correspond to attached communications in the past. [48] It seems that, since Japanese people read between the lines, the victim assumed the email was from the identical person judging prematurely and opened the email.

The 2nd reason is that the contents of the illicit email match the corporate culture and events in Japan. Although many emails related to invoices were found when Emotet was prevalent in October, emails about bonus payments were confirmed in December, which match the period of bonus payments. [48]

IPA published the subject name together with the text actually used in the email. [48] When you receive an email with short text or about matters prevalent in the world, decide whether the email is proper or not utilizing information [50] which is published by IPA or JPCERT/CC. If you cannot decide, do not decide by yourself, contact your boss or a specialist.

5.1.2. Newly spreading ransomware “BitPaymer”

BitPaymer is a kind of ransomware and its activities have been confirmed since around 2017 [51]. Multiple ways of infection have been confirmed and Triple Threat using Emotet [52] and fileless malware attack using PowerShell are its examples [53]. This time, Morphisec, a cybersecurity company from Israel, reported that more than one big enterprise in the auto industry that suffered damage from BitPaymer in August suffered damage from a new attacking method. [54] According to Morphisec, the attacker tries to infect Windows machines with BitPaymer exploiting the vulnerability of Bonjour. Apple published patches that fix more than one vulnerability of Windows version iTunes and iCloud in October 2019. [55] One of the fixed vulnerabilities is the vulnerability of the update component “Bonjour”, where there is a possibility that unintended code might be executed because the execution path executed at update is not surrounded by quotation marks. [54] The flow of infection with BitPaymer exploiting the vulnerability of Bonjour is as follows:

1. The attacker drops BitPaymer with the file name “Program” in the direct directory of C drive of the target Windows machine.
2. Using the automatic update function, Bonjour tries to execute regular files under the folder “C:¥Program Files ¥.....”.
3. However, there is a bug in Bonjour that the execution path of the above folder “C:¥Program Files ¥.....” is not surrounded by quotation marks. Therefore, the execution path is terminated with the space character following “C:¥Program”. As a result, Bonjour executes “C:¥Program”.
4. Since “C:¥Program” is BitPaymer, BitPaymer is executed and infection occurs.

Thus, by storing BitPaymer with the file name “Program” in the direct directory of C drive, the attacker can infect a Windows machine with BitPaymer even if the attacker does not have accounts or execute authority of the machine. [56] This vulnerability can be removed by

applying a patch to Bonjour. However, caution is needed even if Windows version iTunes or iCloud used in the past has been uninstalled. It is because Bonjour remains in the Windows machine and is operating even if iTunes and iCloud are uninstalled. [54] If you uninstalled iTunes or iCloud in the past, install the latest version of iTunes or iCloud to bring Bonjour up-to-date. Or manually delete Bonjour to remove vulnerability. [57]

5.1.3. Ransomware attack targeting healthcare industry

In the 3rd quarter of 2019, ransomware incidents have been occurring frequently in the US as it did in the 1st and 2nd quarter. Among them, ransomware attacks on the healthcare industry have increased rapidly. Ransomware incident cases in the 3rd quarter of 2019 targeting the healthcare industry in the US are shown in Table9.

Table9: Ransomware incidents in the healthcare industry in the US

Date	Target	Summary
October 1	Alabama DCH Health System	The operation was stopped because the system partially stopped due to ransomware attacks. It is said that ransom money was paid and the decryption key was received. The amount of payment is unknown. [58]
October 11	Oregon Monterey Health Center	Medical records were encrypted due to a ransomware attack. Although data were restored, data were deleted from the server. Whether patient information was leaked or not is unknown. [59]
November 17	Virtual Care Provider	Infection with the ransomware "Ryuk". About 80,000 machines were impacted and a 14 million dollar ransom was demanded. [60]
November 20	Missouri Saint Francis Healthcare	Medical records became inaccessible due to a ransomware attack. Although restored since there was a backup copy, some data could not be restored. Payment of ransom was refused. [61]
November 25	Nebraska Great Plains Health	Emails, electronic medical records, etc. became inaccessible due to a ransomware attack. [62]
December 2	New Jersey Hackensack Meridian Health	All 17 associated hospitals and clinics are impacted due to a ransomware attack. The ransom was paid in order to restore the system. The amount of payment is unknown. [63]

December 11	Hawaii Cancer Center of Hawaii	Cancer radiation therapy service at 2 treatment centers were temporarily stopped due to ransomware attacks [64].

In the 3rd quarter, the number of local governments that suffered damage due to ransomware attacks is very few. It is probably because the resolution against ransom payments for ransomware attacks adopted at the United States Conference of Mayors in July 2019 [65] is suppressing ransomware attacks on local governments. There is a possibility that motivation of attackers has been degraded because ransom is not paid and attackers cannot obtain ransom even if the infection with ransomware occurs. It is assumed that attackers were targeting local governments until the 2nd quarter but have changed their target to the healthcare industry due to the above reason. Damage in the healthcare industry due to ransomware attacks not only stops operation but also jeopardizes the lives of patients if early restoration cannot be done. If the importance of lives of patients is compared with the ransom, it is highly possible that medical institutions choose to pay the ransom and restore the system. It is assumed that they were regarded as the perfect targets of attackers because of the above reason.

5.1.4. Conclusion

This chapter introduced the current situation of Emotet and ransomware. This time, small and medium sized enterprises, especially small sized enterprises, in Japan were infected with Emotet. Since measures and training for security at small sized enterprises may be insufficient, it is assumed that many employees of such enterprises opened emails of 3 lines using unsuspicious Japanese. Since emails are used by any organizations, attackers can target a wide range of organizations using emails. Emails are used for spreading malware because they can be received from unspecified third persons. It is recommended to consider migration to chat tools or cloud file sharing service, etc.

Damage from ransomware has been prolonged especially in the US. The result is that while damage on local governments, which had been continuing for many years, seems to have decreased, damage on the health industry has increased. Attackers target organizations with a high probability of paying a ransom. For this reason, it is expected that the target of attackers is changed if the healthcare industry declares that they will not pay a ransom like local governments. In that case, organizations can be the next target if they need prompt restoration since many people are impacted when their system is stopped. For this reason, it is expected that infrastructure companies such as electric power companies and railway companies are targeted. Furthermore, ransomware may become prevalent in Japan as is the

case with Emotet. It is recommended to periodically check not only whether security measures suited for your company's system are taken but also whether measures assuming attacks on your system are stipulated and revise them if needed.

6. Outlook

This chapter describes present trends and outlook based on incidents that occurred in the 3rd quarter of 2019. Methods for attack and exchange for cash after success of an attack are becoming increasingly sophisticated and diversified. Measures for restoration assuming accidents will be of greater need in the future.

Continuously changing ransomware attacks

Methods are being observed where attackers demand ransom threatening to publish stolen information after ransomware encrypts data and files. The attacked organizations not only are forced to stop operation but also receive more pressure to pay ransom, such as handling of data breach and damage to the corporate image, than in past ransom methods. Even if the targeted organization refuses payment of ransom, the attacker can obtain financial benefit by selling stolen data. Because of these things, there is a possibility that methods like this will increase from now on and retailing companies and distribution companies handling cashable information such as credit card information and personal information will be targeted. Responding to changes in attacking method, check the implementation status of your organization's security methods and consider the contents of measures at the time of attack including policies against ransom.

Sophistication of attack method using Emotet

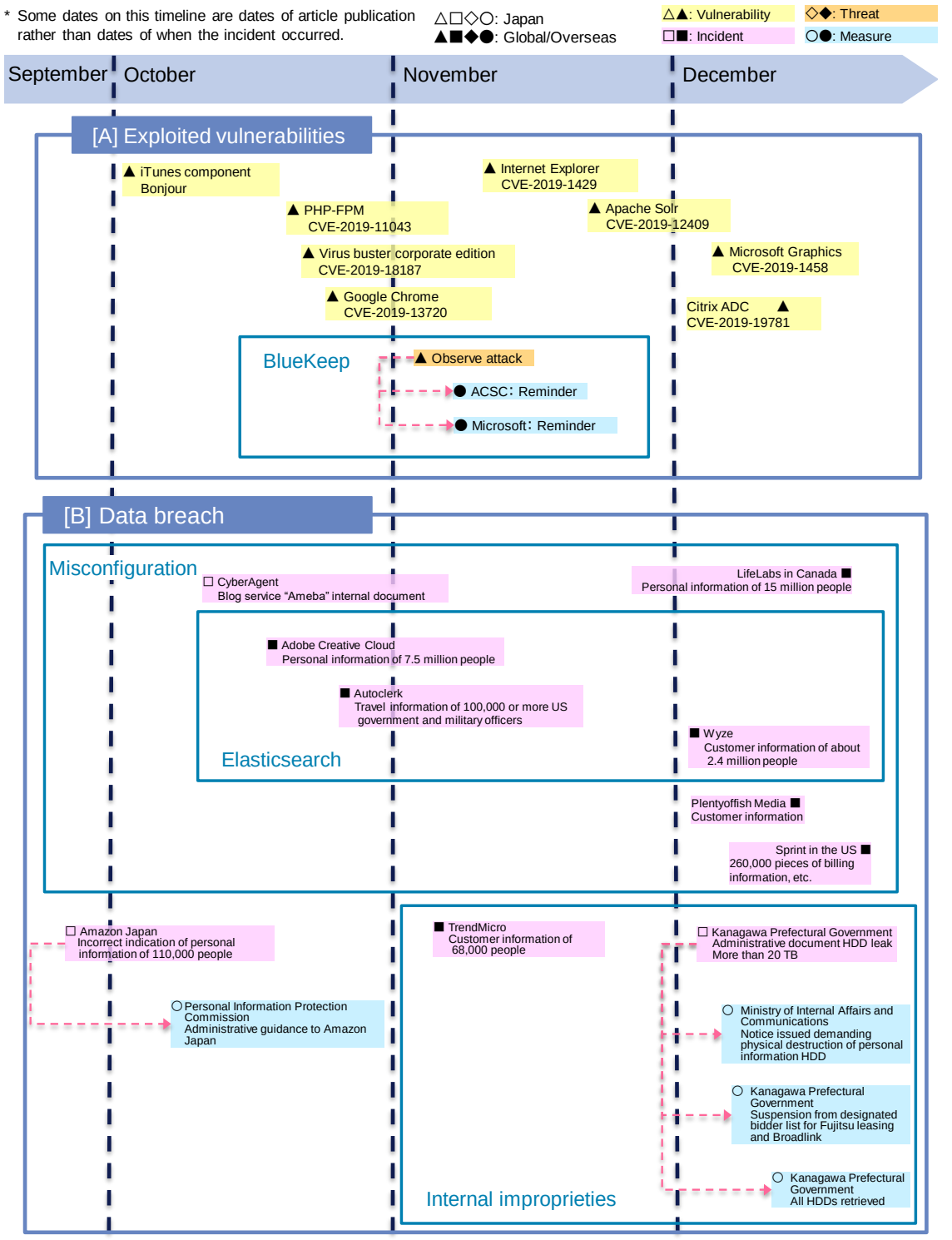
In the 3rd quarter of 2019, damage from infection with Emotet frequently occurred both in Japan and overseas. It is expected that methods of attack after infection will be more sophisticated accompanied with the spread of Emotet infection.

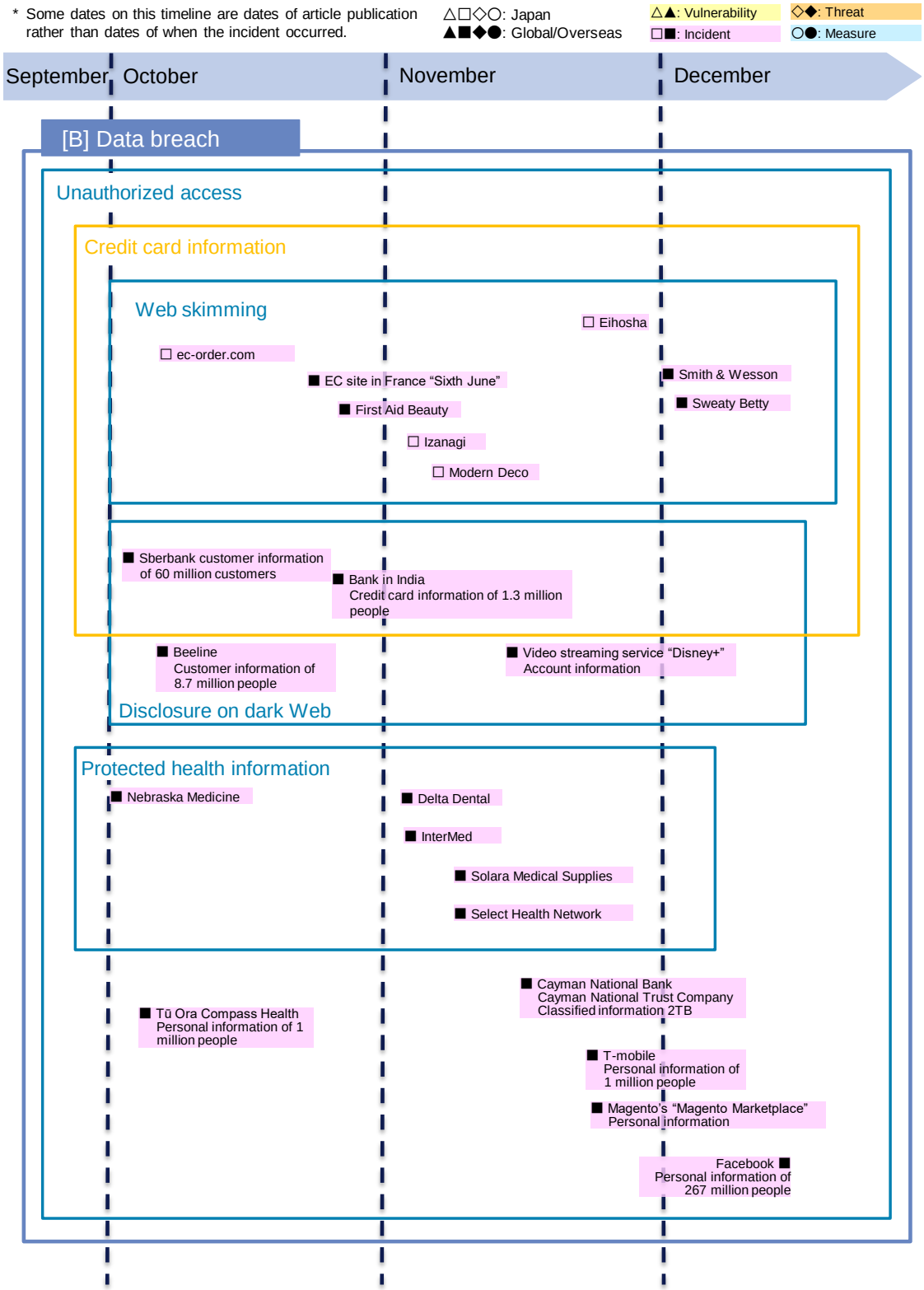
The attacker can easily spoof an employee of the victim organization using email information the attacker acquired by utilizing infection with Emotet. For example, if Emotet is combined with an attack that performs falsification of regular sites such as Web skimming, the user can be more effectively guided to a false site. It is because the user cannot easily realize the fraudulent action since the email seems to be the one from the person with whom the user had communication such as inquiries and the link destination is the regular site. If your computer is infected with Emotet, the most important thing is to send a reminder to people around you in order to prevent secondary damage. On top of that, sorting out the incidents occurring in your organization and measures taken for them, you need to consider what attacks are expected in the future.

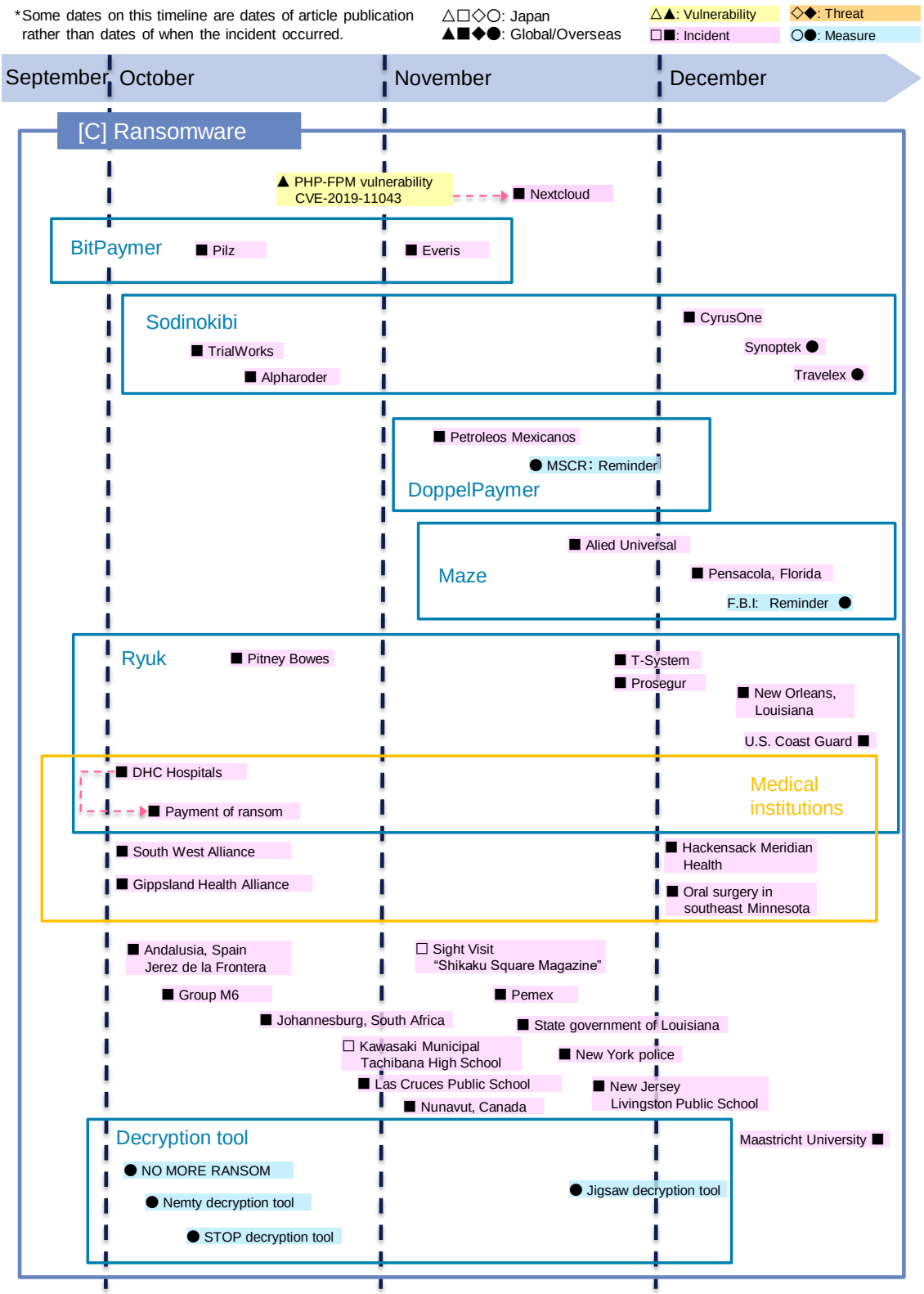
Be careful of attacks exploiting work-style reform and DX

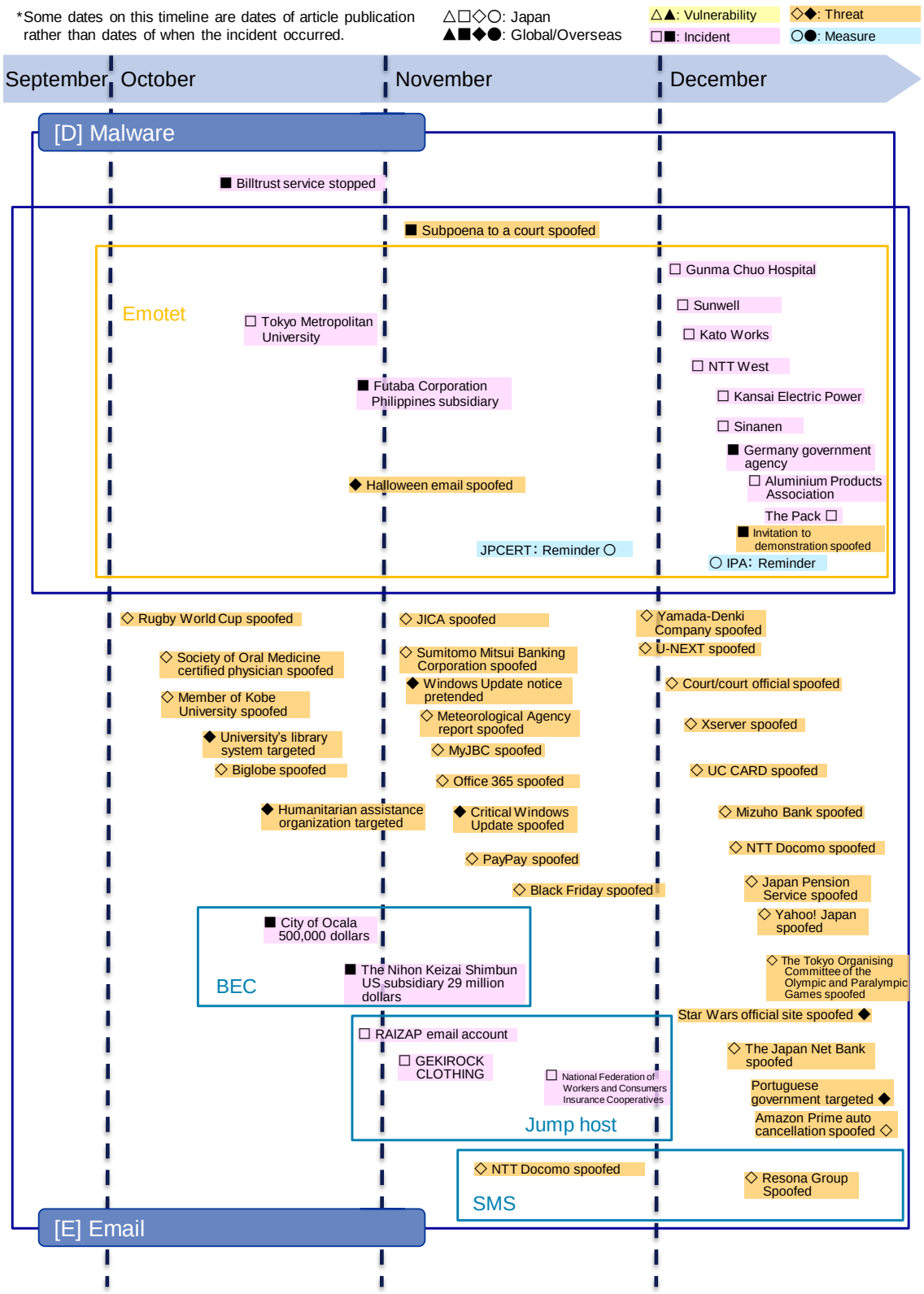
Technologies around society and our work style are changing. There are various vectors such as the Tokyo Olympics, utilization of telework responding to the new-type pneumonia commotion, and promotion of digital transformation (DX) by enterprises. Accompanying these changes is a possibility that the trend of cyberattacks may be changed. Until now, there were many cases using a method of intruding into the inside of organizations with targeted attacks and impinging on their terminals in a cross-sectional way. It is appropriate to think the reason is that important information existed concentratedly on internal networks of organizations. It is expected that attacks aiming to hijack accounts such as SaaS and IDaaS will increase within the context of increased use of cloud services. Design and operation of cloud service authentication and authorization should be strictly conducted. On top of that, proper asset management for information on cloud services is also necessary. It is considered that an attitude to raise both convenience and safety having the correct fear of risks will be of greater need in the future.

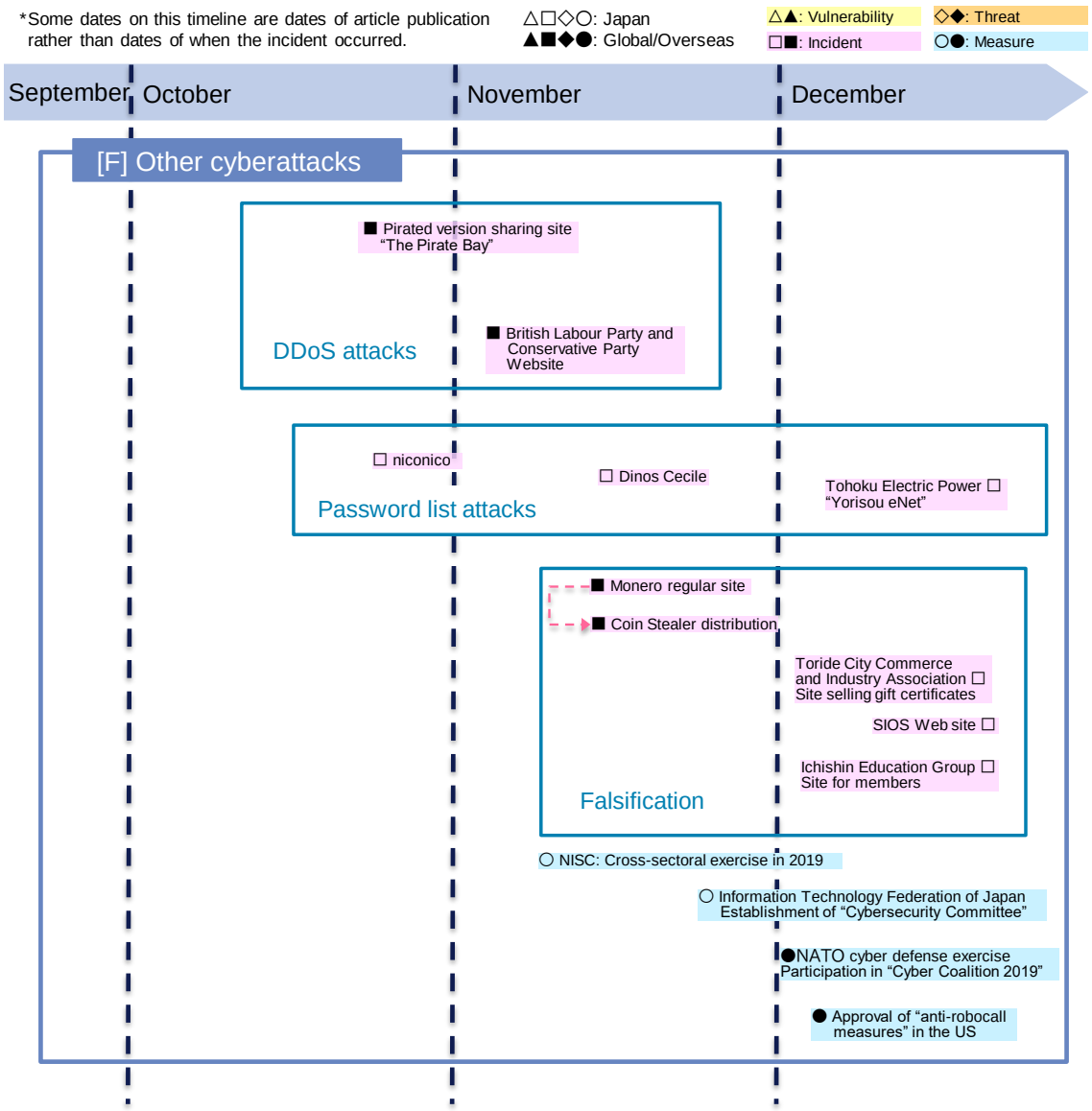
7. Timeline











[1] D. Hardt, "The OAuth 2.0 Authorization Framework," Internet Engineering Task Force, 10 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749.

[2] D. Hardt and M. Jones, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," Internet Engineering Task Force, 10 2012. [Online]. Available: https://tools.ietf.org/html/rfc6750.

[3] 独立行政法人情報処理推進機構, "「 SNS におけるサービス連携に注意！ 」," 独立行政法人情報処理推進機構, 1 10 2012. [Online]. Available: https://www.ipa.go.jp/security/txt/2012/10outline.html.

[4] Microsoft, "Microsoft 公式 - 家庭向けおよび一般法人向け Office 製品の比較," Microsoft, 2020. [Online]. Available: https://products.office.com/ja-jp/compare-all-microsoft-office-products?&activetab=tab:primaryr2.

[5] O. Tsarfati, "BlackDirect: Microsoft Azure Account Takeover," CyberArk Software Ltd., 2 12 2019. [Online]. Available: https://www.cyberark.com/threat-research-blog/blackdirect-microsoft-azure-account-takeover/.

[6] CyberArk Software Ltd., "Microsoft and Azure Account Takeover," CyberArk Software Ltd., 2019. [Online]. Available: https://black.direct/.

[7] M. Tyler, "Phishing Campaign Uses Malicious Office 365 App," PhishLabs, 9 12 2019. [Online]. Available: https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset.

[8] CyberArk Software Ltd., CyberArk Software Ltd., 2019. [Online]. Available: https://black.direct/videos/blackdirect_poc.mp4.

[9] 朝日新聞デジタル, “【独自】行政文書が大量流出　納税記録などのＨＤＤ転売,” 6 12 2019. [オンライン]. Available: https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html?iref=pc_extlink.

[10] 日経ビジネス, “神奈川HDD転売、元社員は3904個を販売　企業・官公庁に飛び火も,” 10 12 2019. [オンライン]. Available: https://business.nikkei.com/atcl/gen/19/00002/121000948/?P=2&mds.

[11] ITmedia, “HDD転売問題のブロードリンク、従業員30人に解雇通知　社長も退任の意向,” 8 1 2020. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2001/08/news137.html.

[12] ZDNet, “トレンドマイクロ、内部不正による個人ユーザーの情報流出を発表,” 6 11 2019. [オンライン]. Available:

https://japan.zdnet.com/article/35144967/.

[13] IPA, “組織における内部不正対策,” 14 7 2015. [オンライン]. Available: https://www.ipa.go.jp/files/000047237.pdf.

[14] ブロードリンク, “今後の再発防止策,” 9 12 2019. [オンライン]. Available: https://www.broadlink.co.jp/info/pdf/20191209-03-press-release.pdf.

[15] 朝日新聞デジタル, “ブロードリンク元社員を再逮捕　会社からHDD窃盗容疑,” 22 1 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN1Q3H0MN1QUTIL005.html.

[16] IPA, “組織における内部不正防止ガイドライン,” 1 2017. [オンライン]. Available: https://www.ipa.go.jp/files/000057060.pdf.

[17] Hy-Vee, “Notice of Data Breach,” 3 10 2019. [オンライン]. Available: https://www.hy-vee.com/corporate/news-events/announcements/notice-of-payment-card-data-incident-3/.

[18] Krebs on Security, “Sale of 4 Million Stolen Cards Tied to Breaches at 4 Restaurant Chains,” 26 11 2019. [オンライン]. Available: https://krebsonsecurity.com/2019/11/sale-of-4-million-stolen-cards-tied-to-breaches-at-4-restaurant-chains/.

[19] BleepingComputer, “U.S. Food Chain Alerts Customers of Payment Card Incident,” 28 10 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-food-chain-alerts-customers-of-payment-card-incident/.

[20] VISA, “ATTACKS TARGETING POINT-OF-SALE AT FUEL DISPENSER MERCHANTS,” 11 2019. [オンライン]. Available: https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf.

[21] VISA, “CYBERCRIME GROUPS TARGETING FUEL DISPENSERMERCHANTS,” 12 2019. [オンライン]. Available: http://click.broadcasts.visa.com/xfm/?30761/0/0624013ddc6f39785bf56d504f3b812e/lonew.

[22] security affairs, “Payment card breach potentially impacts all locations of Wawa convenience store,” 20 12 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/95412/data-breach/wawa-payment-card-breach.html.

[23] VMware Carbon Black, “4 Point-of-Sale Security Flaws that Jeopardize Customer Data,” 2 10 2014. [オンライン]. Available: https://www.carbonblack.com/2014/10/02/4-point-of-sale-security-flaws-that-jeopardize-customer-data/.

[24] 株式会社 リンク, “PCI P2PE(PCI Point-to-Point Encryption)とは?,” 27 4 2016. [オンライン]. Available: https://pcireadycloud.com/blog/2016/04/27/862/.

[25] ScanNetSecurity, “Target のレジがマルウェアに感染、4,000 万のバンクカードを吸い上げる,” 23 1 2014. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2014/01/23/33411.html.

[26] カスペルスキー, “米国、EMV仕様クレジットカードへの移行で詐欺が増加,” 17 5 2016. [オンライン]. Available: https://blog.kaspersky.co.jp/us-emv-transition-increases-fraud/11188/.

[27] 日本クレジットカード協会, “ＩＣクレジットカードに関する消費者意識調査,” 27 11 2019. [オンライン]. Available: http://www.jcca-office.gr.jp/topics/topics_77.html.

[28] The PHP Group, "Sec Bug #78599 env_path_info underflow in fpm_main.c can lead to RCE," 26 9 2019. [Online]. Available: https://bugs.php.net/bug.php?id=78599.

[29] Help Net Security, "PHP RCE flaw actively exploited to pop NGINX servers," 28 10 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/10/28/cve-2019-11043/.

[30] NGINX, "Addressing the PHP-FPM Vulnerability (CVE-2019-11043) with NGINX," 29 10 2019. [Online]. Available: https://www.nginx.com/blog/php-fpm-cve-2019-11043-vulnerability-nginx/.

[31] NTTデータ先端技術株式会社, "PHP-FPMに含まれるリモートコード実行に関する脆弱性（CVE-2019-11043）についての検証レポート," 6 11 2019. [Online]. Available: http://www.intellilink.co.jp/article/vulner/191106.html.

[32] BLEEPING COMPUTER, "New NextCry Ransomware Encrypts Data on NextCloud Linux Servers," 15 11 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers/.

[33] Nextcloud, "Urgent security issue in NGINX/php-fpm," 24 10 2019. [Online]. Available: https://nextcloud.com/blog/urgent-security-issue-in-nginx-php-fpm/.

[34] Cisco, "Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability," 24 9 2019. [Online]. Available: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd.

[35] Help Net Security, "Unpatched Android flaw exploited by attackers, impacts Pixel, Samsung, Xiaomi devices," 4 10 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/10/04/cve-2019-2215/.

[36] Security Affairs, "Hackers continue to exploit the Drupalgeddon2 flaw in attacks in the wild," 8 10 2019. [Online]. Available: https://securityaffairs.co/wordpress/92239/malware/drupalgeddon2-campaign.html.

[37] NTT DATA, "グローバルセキュリティ動向四半期レポート 2019年度第2四半期," 29 11 2019. [Online]. Available: https://www.nttdata.com/jp/ja/news/information/2019/112900/.

[38] NATIONAL SECURITY AGENCY, "MITIGATING RECENT VPN VULNERABILITIES," 7 10 2019. [Online]. Available: https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/1/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.pdf.

[39] Trend Micro, "【注意喚起】ウイルスバスター コーポレートエディションの脆弱性(CVE-2019-18187)を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い," 28 10 2019. [Online]. Available: https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=3592.

[40] Google, "Stable Channel Update for Desktop," 21 10 2019. [Online]. Available: https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html.

[41] CERT NZ, "Critical vulnerability in Microsoft remote desktop services," 5 11 2019. [Online]. Available: https://www.cert.govt.nz/it-specialists/advisories/vulnerability-microsoft-rdp-services/.

[42] Security Affairs, "Capesand is a new Exploit Kit that appeared in the threat landscape," 8 11 2019. [Online]. Available: https://securityaffairs.co/wordpress/93577/malware/capesand-exploit-kit.html.

[43] BLEEPING COMPUTER, "Magento Urges Users to Apply Security Update for RCE Bug," 11 11 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/magento-urges-users-to-

apply-security-update-for-rce-bug/.

[44] Security Affairs, "Microsoft Patch Tuesday updates fix CVE-2019-1429 flaw exploited in the wild," 13 11 2019. [Online]. Available: https://securityaffairs.co/wordpress/93787/hacking/cve-2019-1429-flaw-fixed.html.

[45] Security Affairs, "Microsoft fixes CVE-2019-1458 Windows Zero-Day exploited in NK-Linked attacks," 11 12 2019. [Online]. Available: https://securityaffairs.co/wordpress/94936/hacking/microsoft-fixes-cve-2019-1458.html.

[46] 尚. 大谷, 義. 小林, 眞. 大石 , 大. 山下, “グローバルセキュリティ動向四半期レポート　2019年度第1四半期,” 株式会社NTTデータ, 29 8 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_1q_securityreport.pdf.

[47] 岡本勝之, “引き続き国内で拡大する「EMOTET」の脅威,” TREND　MICRO, 27 1 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23648.

[48] 独立行政法人情報処理推進機構 セキュリティセンター, “「Emotet」と呼ばれるウイルスへの感染を狙うメールについて,” 独立行政法人情報処理推進機構 セキュリティセンター, 31 1 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[49] 時事通信社, “菅官房長官、ＰＣウイルスで注意喚起　「エモテット」,” 時事通信社, 28 11 2019. [オンライン]. Available: https://www.jiji.com/jc/article?k=2019112800997&g=pol.

[50] JPCERT/CC　コーディネーションセンター, “マルウエア Emotet の感染に関する注意喚起,” JPCERT/CC　コーディネーションセンター, 10 12 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190044.html.

[51] BBC, “Ransomware behind NHS Lanarkshire cyber-attack,” BBC, 28 8 2017. [オンライン]. Available: https://www.bbc.com/news/uk-scotland-glasgow-west-41076591.

[52] ウェブルート株式会社, “ウェブルート「最も危険なマルウェア2019」を公表,” ウェブルート株式会社, 17 12 2019. [オンライン]. Available: https://www.webroot.com/jp/ja/about/press-room/releases/2019.

[53] M. R. Lopez, “Spanish MSSP Targeted by BitPaymer Ransomware,” McAfee, 8

11 2019. [オンライン]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/.

[54] M. Gorelik, “APPLE ZERO-DAY EXPLOITED IN NEW BITPAYMER CAMPAIGN,” Morphisec, 10 10 2019. [オンライン]. Available: https://blog.morphisec.com/apple-zero-day-exploited-in-bitpaymer-campaign.

[55] Apple, “iTunes for Windows 12.10.1 のセキュリティコンテンツについて,” Apple, 2 12 2019. [オンライン]. Available: https://support.apple.com/ja-jp/HT210635.

[56] D. GOODIN, “Attackers exploit an iTunes zeroday to install ransomware,” Ars Technica, 11 10 2019. [オンライン]. Available: https://arstechnica.com/information-technology/2019/10/attackers-exploit-an-itunes-zeroday-to-install-ransomware/.

[57] C. Cimpanu, “Ransomware gang uses iTunes zero-day,” ZDNet, 10 10 2019. [オンライン]. Available: https://www.zdnet.com/article/ransomware-gang-uses-itunes-zero-day/.

[58] M. Garrity, “3 Alabama hospitals halt admissions after ransomware attack,” Becker's healthcare, 2 10 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/3-alabama-hospitals-halt-admissions-after-ransomware-attack.html.

[59] M. Garrity, “Oregon medical center EHR encrypted in ransomware attack,” Becker's Healthcare, 17 10 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/oregon-medical-center-ehr-encrypted-in-ransomware-attack.html.

[60] M. Garrity, “Virtual Care Provider target in $14M ransomware attack, leaving patient records inaccessible,” Becker's Healthcare, 25 11 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/virtual-care-provider-target-in-14m-ransomware-attack-leaving-patient-records-inaccessible.html.

[61] M. Garrity, “Missouri health system alerts patients of ransomware attack,” Becker's Healthcare, 21 11 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/missouri-health-system-alerts-patients-of-ransomware-attack.html.

[62] M. Garrity, “Great Plains Health cancels nonemergency procedures after ransomware attack,” Becker's Healthcare, 27 11 2019. [オンライン]. Available:

https://www.beckershospitalreview.com/cybersecurity/great-plains-health-cancels-nonemergency-procedures-after-ransomware-attack.html.

[63] J. Drees, “Hackensack Meridian paid ransom for cyberattack that shut down computer network,” Becker's Healthcare, 13 12 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/hackensack-meridian-paid-ransom-for-cyberattack-that-shut-down-computer-network.html.

[64] M. Garrity, “Cancer radiation treatment halted after ransomware attack at Hawaii center,” Becker's Healthcare, 12 12 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/cancer-radiation-treatment-halted-after-ransomware-attack-at-hawaii-center.html.

[65] The United States Conference of Mayors, “87th Annual Meeting Opposing Payment To Ransomware Attack Perpetrators,” The United States Conference of Mayors, 9 7 2019. [オンライン]. Available: http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%20and%20Social%20Justice.

NTT DATA
Trusted Global Innovator

Published on February 28, 2020

NTT DATA Corporation
Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Ryo Hoshino / Etsuo Suzuki / Kenshiro Itayama / Tomohiro Ito / Takayuki Kato /
Kazuki Shimizu