NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

4th 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 NTTDATA_CERT on quarterly global trends from its own perspective based on cybersecurity-related information collected in the period.

Spreads of coronavirus and phishing attacks

The number of phishing attacks is increasing with the spread of the novel coronavirus. There are many phishing cases by a cyber attack group known as “Roaming Mantis,” which uses unauthorized applications that spread malware by assuming a false map where people can check the status of coronavirus spread or sending SMS messages with false information of distributing free face masks. Coronavirus-related phishing attacks are characterized by users who become a victim of the phishing fraud before they know it since attackers use artful methods that can take advantage of people’s psychological state of anxiety. However, you can prevent yourself from fraud by knowing the characteristics of the phishing methods and devising ways for senders of alerts to send accurate information without fail. The following are the points to be noted for information receivers to prevent phishing fraud.

Lateral movement

In January 2020, cyber attacks to four defense-related Japanese companies took place. One of the companies was Mitsubishi Electric Corporation, whose case is considered to have been an advanced cyber attack as the damage reached wider areas through lateral movement even in an environment where it was assumed that measures had been taken for methods used frequently by attackers. For such attacks, assuming intrusions, it is effective to take measures focusing on the end point where confidential information is stored, which is the target of attackers. Government organizations and defense-related companies are frequent targets for such advanced cyber attacks, and their related organizations and clients are likewise facing the same threat. It is therefore important to keep a lookout for attacks not only on direct targeted organizations and companies but also on their related organizations and clients which comprise the supply chain.

Data exposing ransomware attacks

Damage from ransomware including Maze and Sodinokibi have been a big topic in the US.

In previous cases of ransomware damage, ransom was demanded in exchange for recovering encrypted files. There have been more data exposing ransomware attacks in which ransom is demanded in exchange for not exposing data stolen from an organization.

Once information is stolen by data exposing ransomware, it is difficult to recover it.

Therefore, it is recommended to assume that the stolen information has already been breached and try to take measures for restoration.

Outlook

In the 4th quarter of 2019, damage from data exposing ransomware which is targeted at companies occurred frequently. Data exposing ransomware attacks can cause significant damage and it is expected that their target will spread to individuals. In particular, coronavirus continues to be a topic of great concern worldwide and it is necessary to be cautious about attacks which take advantage of the news. If you sense something is suspicious, be sure to protect yourself against cyber attacks by seeking objective opinions of third parties rather than assessing the situation based on your own assumptions.

The security level can become lower if the budget is reduced as the economy worsens and the planned security measure is ceased or postponed, or the present security operation is downsized. As the number of cyber attacks is increasing, it is recommended to compile a budget to secure necessary security level and take measures.

2. Featured Topics

2.1. Spreads of coronavirus and phishing attacks

Since December 2019, outbreaks of the new coronavirus infectious disease have been showing explosive spreads all over the world. The number of new cases, comments of healthcare workers who support healthcare facilities in critical condition, economic measures, protest movements against stagnated economic situations are reported daily, and movements that are peculiar to an “emergency situation” have also been identified in cyberspace.

When the world falls into a panic after the occurrence of a large-scale natural disaster such as an earthquake, typhoon or hurricane, terrorism or pandemic caused by an infectious disease like the present situation, malware that takes advantage of the situation spreads and the number of targeted attacks and phishing attacks increases. This is aimed at stealing authentication information or money by taking advantage of people’s sense of anxiety and good will for support.

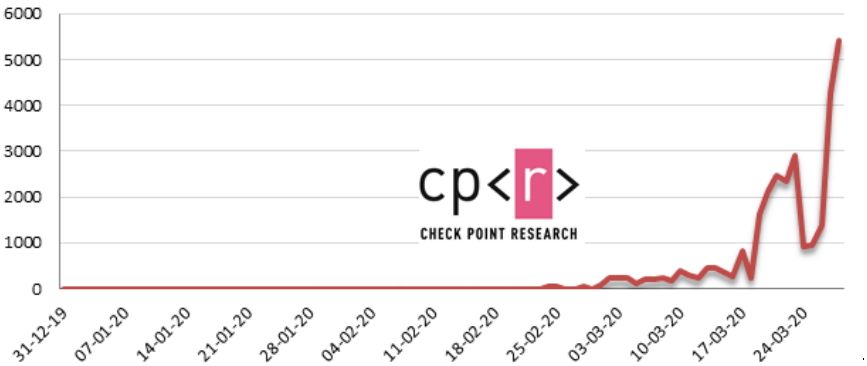


Figure 1: Changes in the number of cyber attacks related to coronavirus [1]

Figure 1 is a graph showing an increase in the number of various attacks related to coronavirus, which were detected by a solution released by Check Point. About 84% of the detected attacks were phishing attacks. KnowBe4 revealed that, as a result of the phishing drill campaign conducted between January and March 2020, the number of victims of the phishing drill Emails which were related to coronavirus was the second largest. It is reported that this number followed the phishing drill Emails which notified an immediate password check. [2] The number of phishing Email attacks related to coronavirus has increased by six times in 2020. The company commented that it is necessary to exercise caution as the number of phishing attacks related to coronavirus will increase, taking advantage of the psychology of people who seek for various information.

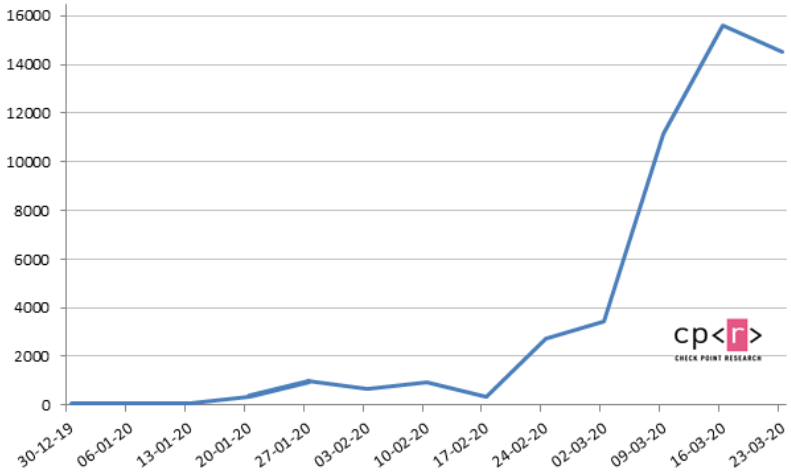


Figure 2: Changes in the number of new domain registrations (per week) related to coronavirus [1]

Figure 2 is a graph showing an increase in the number of new domain registrations related to coronavirus, which was compiled by Check Point. The values in the vertical axis show the numbers of new domains registered. This shows that, after January 2020, a total of more than 51,000 domains have been registered. Domains registered within the last 2 weeks include malicious domains (0.4%) and suspicious domains (9%). When you search a coronavirus-related website, around 10% of the results shown might be potential sites with risks.

This report considers coronavirus-related phishing attacks in which users could become a victim before they know it as the attackers use artful methods.

2.1.1. Spread of unauthorized applications

There are several ways for attackers to spread malware. There is an increasing number of malware infection cases which spread when users download an unauthorized application (which appears to be authorized) on a phishing site without noticing it.

“Unauthorized applications under Coronavirus Crisis”

As the infection from the coronavirus spreads, various applications related to “the novel coronavirus infection map” have been distributed, where the epidemic situation of the virus can be checked. However, some of them are unauthorized applications pretending to be an infection map. If you start an unauthorized application, your smart phone would be locked. Virtual currency is demanded in exchange for unlocking the phone, and malware known as AZORult or a subvariety is installed on your PC or smart phone to steal private information. [3] [4] AZORult is a Trojan for commercial use generally sold in underground forums in Russia in order to obtain information. [5] It spreads through exploit kits and phishing emails,

and it is known to steal IDs, passwords, email authentication information, cookies, browser history and cryptocurrency, and also function as a back door. [6] AZORult was used for a spear phishing campaign taken place in North America in July 2018. In Japan, a spread was found in November 2018 through phishing emails which pretended to be a tsunami alarm sent by the Japan Meteorological Agency to people in the Tohoku region. [7] Table 1 shows examples of unauthorized applications related to coronavirus infection maps.

Table 1: Examples of unauthorized applications related to coronavirus infection maps

Name of applications	Target	Summary
Corona-Virus-Map[.]com **[3]**	Windows	・When you access the phishing site "Corona-Virus-Map[.]com," pretending to be a website for information on coronavirus infections created by Johns Hopkins University, malware requests you to download an execution file named "Corona-Virus-Map[.]com.exe." [8] ・If you download and install the execution file, malware including AZORult is installed and AZ ORult starts. Then, AZORult is registered as a startup task in the task scheduler. ・The malware displays coronavirus infection map, while stealing information in the background from OS or browsers and sending it to the C&C server.
Corona live 1.1 **[9]**	Android	・An unauthorized application pretending to be the coronavirus infection map which is published by Johns Hopkins University ・It is available on a website, not in the Google Play Store. ・It is notified that no special access authorization is necessary when the application is started for the first time. Then, access authorization to location information and a smart phone camera is requested in order to "enable tracking of the coronavirus spread (false)." ・Attackers use the access authorization obtained to record users' location, photos and videos without a permission and steal personal information on the device. ・An application developed and distributed to disguise itself as the spyware "SpyMax" [1].

Coronavirus Tracker **[10]**	Android	・It is available on a website with the domain Coronavirusapp[.]site, not in the Google Play Store. ・If you access the Coronavirusapp[.]site, you are encouraged to install an application that displays a coronavirus epidemic map called "Coronavirus Tracker." ・If you accept the installation, ransomware called CovidLock is installed on the user's smart phone and all operations will be locked. To unlock the phone, you will be asked to give some bitcoins. ・The installation site has been closed as of today.

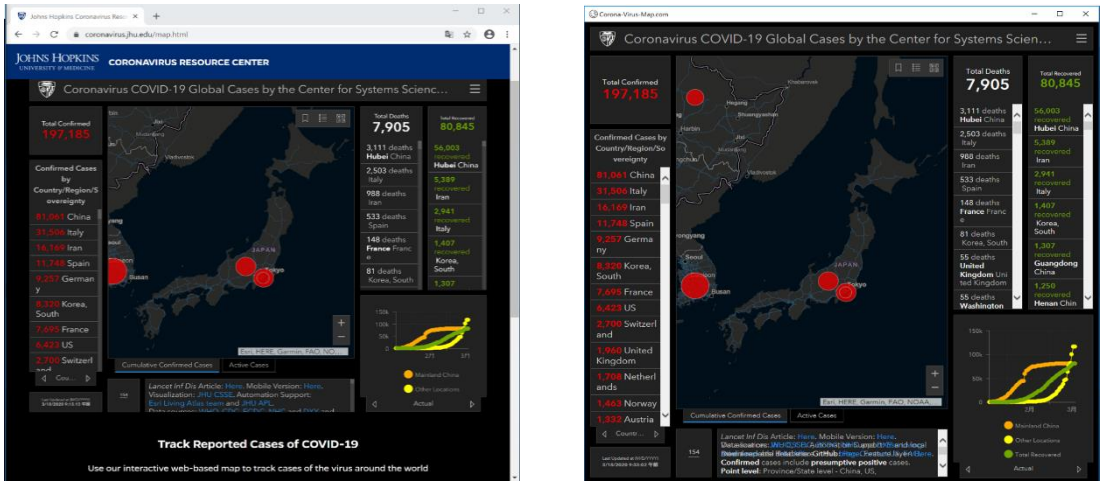


Figure 3: Authorized infection map (left) and fake infection map (right) [11]

Figure 3 compares the display of the authorized website of Johns Hopkins University and that of malware "Corona-Virus-Map[.]com.exe." Figure 3To display the right-side infection map, you need to access the phishing site "Corona-Virus-Map[.]com" and download and install the execution file. This is the major difference from the authorized website. However, because the attacker developed and distributed the application which displays a screen identical to the authorized website using the aggregate data published on GitHub by Johns Hopkins University by creating a phishing site with the domain name "Corona-Virus-Map[.]com" which appears to be real, users do not suspect that the application is suspicious and download and install malware pretending to be an infection map application. After having installed the malware, users do not realize that the malware steals their information as it displays the updated infection map using data published by Johns Hopkins University.

2.1.2. Spread of Roaming Mantis activities

"Roaming Mantis" is a phishing attack group targeting PCs and smart phones. Its activities have been identified taking advantage of the spread of the novel coronavirus.

"Roaming Mantis under Coronavirus Crisis"

The number of SMS messages sent by Roaming Mantis which pretend to "distribute free face masks" is increasing with the spread of coronavirus. Phishing attacks which use SMS messages are known as "smishing". In the same method as the smishing of absence notification by senders who pretend to be a delivery company, which was mentioned in the 2018 report, smishing cases using the words "free face mask distribution" have been reported [12] [13].

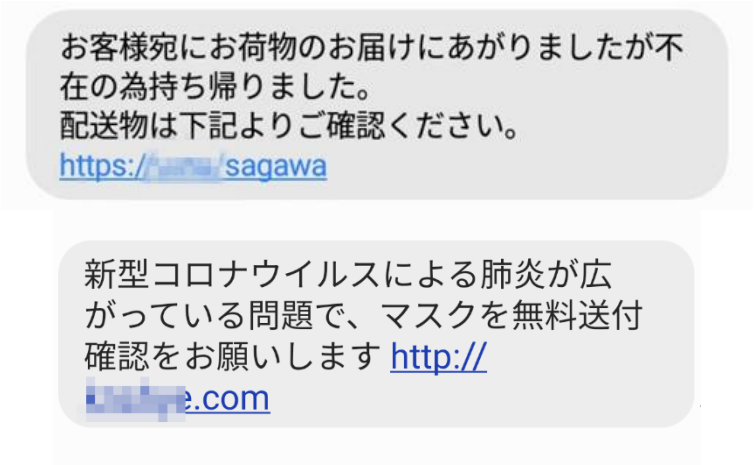


Figure 4: Example of an SMS message (above) pretending to be an absence notification from a delivery company [14] **Example of an SMS message pretending to distribute free face masks (bottom)** [15]

The linked page which is led by smishing is called a landing page. The landing page of the above URL is an unauthorized website which tries to steal authentication information of Apple ID, etc. or a website which encourages installation of an unauthorized application. Such coronavirus-related smishing cases started to appear in early February when various events began to be canceled due to the outbreak of domestic infection cases. Roaming Mantis has immediately replaced existing attacks by changing message contents to a topical subject. It is necessary to continue to pay attention to smishing as it uses artful contents which focus in on people's psychological state of anxiety and interests.

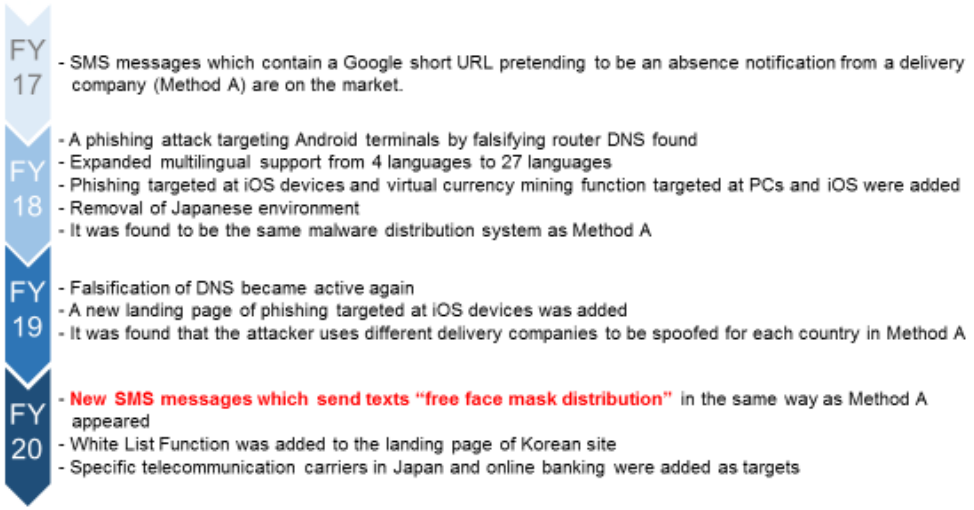


Figure 5： Trends related to Roaming Mantis [16] [17] [18] [19] [20]

Figure 5 shows trends related to the attack group Roaming Mantis. Roaming Mantis has expanded the target of attacks by immediately changing target languages and devices. Looking at a series of events, it is considered that Roaming Mantis had first checked the effect of attacks in a limited area, South Korea, and then expanded the target area of attacks to successfully deceive target users.

In 2020, Roaming Mantis added two new functions. One of them is the White List Function for phishing sites [20]. This function requests users to input their mobile phone numbers when they access the landing page. An unauthorized application is distributed only when the phone number exists in the attacker's list. This hinders investigation teams from obtaining samples. Although only South Korea is targeted at present, it is likely that the group will expand the area of attacks while dodging investigations and try to advance their attacking tactics.

Another function added to malware for smart phones is a function to collect device information. The malware added a function which leads users to a matching phishing site when it detects a specific bank application or use of a specific mobile phone carrier in infected smart phones [21]. It is clear that Roaming Mantis is greatly motivated to obtain money from attacks.

It is expected that the number of coronavirus-related acts for money will increase in the future, including those which are associated with the 100,000 yen handout given from the national government to each resident and the distribution of free face mask coupons by local governments. For example, there can be a method of smishing and phishing attacks which send a message saying "confirm your account with regard to the 100,000 yen handouts" and an unauthorized URL falsifying confirmation, and try to steal account information in the linked website. In Germany, there were a series of false applications by attackers who pretend to be applicants using people's private information they stole

through a phishing site of the subsidy application website and try to receive the subsidy in a fake account from the authorized application website [22]. In Japan's authorized subsidy application site, it requests to input bank account information to receive the subsidy. Attackers create a phishing site of the subsidy application site and it may request your PIN code as well as your account information in order to illegally transfer money from the account through online banking. It is necessary to take caution as they use artful tactics to attack two-factor authentication including one-time passwords used frequently in online banking.

2.1.3. Conclusion (measures)

Damage from phishing attacks can be prevented by ensuring that people know appropriate measures. In order to avoid damage from a false application which pretends to be the "novel coronavirus infection map" and smishing by Roaming Mantis, which is mentioned here, points to be noted from the viewpoint of senders and receivers of information are listed below.

Points to be noted by information senders

It is necessary for information senders not to send misleading information taking into account the increasing number of phishing attacks related to coronavirus and consider ways to protect their information transmitting media from being used by smishing and phishing attacks. In particular, officials of government agencies and local governments should be able to prove the "authenticity" of the message in order to transmit accurate information to the public without fail. First, it is better to avoid using SMS messages as information transmission media. SMS has no function to block unauthorized senders and anyone can send smishing messages. Therefore, it tends to be abused easily. Obtaining an SSL server certificate is one countermeasure for phishing sites. There are three types of SSL server certificate: "Domain Validation (DV)," "Organization Validation (OV)" and "Extended Validation (EV)," which is decided depending on the validation level. The "Extended Validation" SSL server certificate which requires the strictest screening of the three validates is effective as a countermeasure for phishing attacks. It enhances the credibility of a website as it can certify the existence of the website operator [23].

Points to be noted by information receivers

Many coronavirus-related websites, applications emails have appeared on the market. Although there are many which do send correct information, attackers develop malicious websites by exploiting this environment. People are spending more time at home and tend to use the Internet longer. It is necessary to be aware of the fact that around 10% of the websites which provide coronavirus-related information might have potential risks. Your state of mind might be unstable as you refrain from going out or change your working style. Be careful not to click a URL written in emails and SMS messages carelessly more than

usual. Specifically, messages which appear to be urgent requesting you to check the content should be a red flag, so do not click the link in the text. Table 2 summarizes the points to be noted for information receivers to avoid phishing fraud.

Table 2: Points to be noted to prevent phishing fraud

Points to be noted by information receivers	Reason (attacker's intention)
• Install any applications from an official store. Do not install an application directly from a website or a third party app store. • Limit downloads of applications (including files) to the minimum essentials and install them after confirming access authority.	• Unauthorized applications which contain malware such as Coronavirus Tracker and Corona live 1.1 are distributed in phishing sites and third party app stores to avoid security screening of official app stores.
• Do not click a URL included in emails and SMS messages carelessly. Be especially careful if the URL is shortened. Specifically, messages which appear to be urgent requesting you to check the content should be a red flag, so do not be click the link in the text. • It is effective to check the linked URL before clicking it. If you are a PC user, a URL is shown if you hover the mouse cursor over the linked text on the browser (hover function).	• The attacker uses messages which include artful text and URLs to let users connect to phishing sites. • SMS has no function to block unauthorized senders and anyone can send smishing messages. • Short URLs can attract users' access to fraudulent sites without noticing it because they can hide the domain name in the link.
• Use the updated version of OS and applications with fixed vulnerability.	• Attackers exploit the vulnerability of applications and OS and try to infect devices with malware.
• Do not use free Wi-Fi access points since you cannot verify their safety.	• Attackers prepare a free Wi-Fi access point and lead users who access a website on PCs and smart phones connected to the point to phishing sites.

2.2. Lateral movement

In recent years, many companies have been targeted for cyber attacks. In January 2020, cyber attacks to four defense-related Japanese companies took place. Of the four, Mitsubishi Electric Corporation (hereinafter referred to as Mitsubishi Electric) was equipped with multi-layer protective function in the information system environment and had implemented maintenance and operation of the emergency response system for incident occurrence. However, caution information designated by the Ministry of Defense (information which requires the presentation of a written pledge and thorough maintenance at the time of lending) and 8122 personal information might have been leaked [24] [25] [26].

This incident is considered to have been caused partly by the following acts (hereinafter referred to as lateral movement) which could increase the number of breaches in an organization.

- Expansion of breach from one point to multiple points in China
- Breach from a terminal at one point to anti-virus management server of domestic points in China
- Expansion of breach from anti-virus management server to several domestic points in China

We will consider what is a lateral movement attack and what kind of measures are effective for it.

2.2.1. About lateral movement

Lateral movement is an act of expanding the scope of breach in an organization in order to approach important assets targeted by APT (Advanced Persistent Threat) attacks. Lateral movement uses the following methods in Table Table 3 [27].

Table 3 : Methods of lateral movement

	Category	Summary
1	Exploitation of vulnerability	・ Exploit the vulnerability of general services such as RDP, SMB, print spooler service, etc. used by the machine in OA environments and internal systems, and service used by servers including MySQL, etc. and illegally access other machines.
2	Exploitation of OS standard functions/exploitation of OS vendor's genuine tools	・ Exploit RDP, SSH, SMB/Windows Admin Share, WinRM, PsExec, WMI, etc. using existing accounts and illegally access other machines ・ Register malware as a task using [schtasks] and [at] in machines

3	Exploitation of substitutive authentication factor	・ Bypass ordinary identification and authentication by exploiting substitutive authentication factors such as password hash and a ticket for Kerberos authentication and illegally access other machines
4	Exploitation of management tools	・ Exploit management and monitoring tools and illegally access other machines

We will guess how lateral movement attacks were carried out in the Mitsubishi Electric incident from Mitsubishi Electric's press release, etc. We guessed based on the past cyber attack cases for the parts which could not read from press releases. As a result, it is assumed that this cyber attack was carried out in a flow as below Figure 6 Figure 6 [24] [28]:

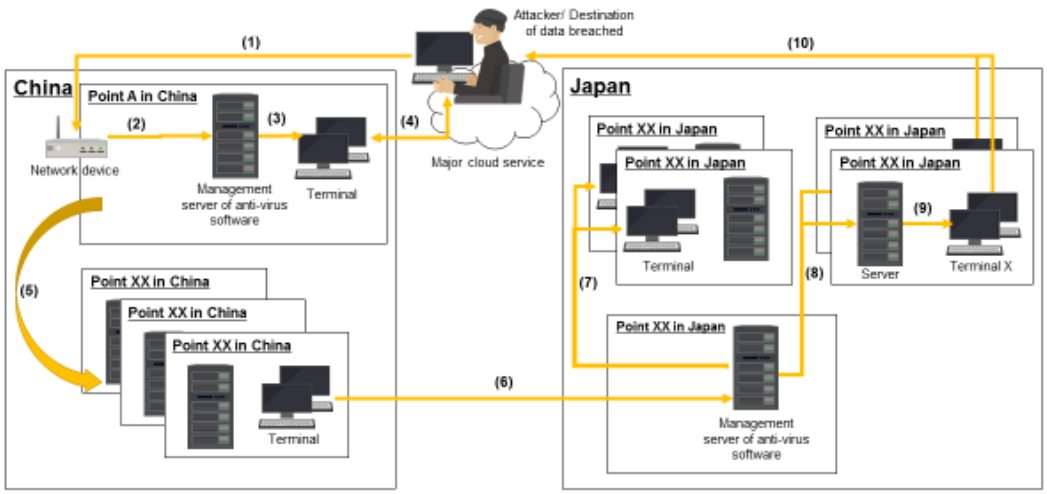


Figure 6: Flow of cyber attack to Mitsubishi Electric (image)

① Intrusion into network devices with inadequate management at Point A in China
② Intrusion into the management server by attacking the unpublished vulnerability of the server of anti-virus software at Point A
③ Distribution of Dropper Malware to several terminals at Point A by exploiting the pattern file update function of the management server
④ There was a vulnerability in the anti-virus software in the said terminal and the anti-virus software started Dropper Malware which was replaced with the authorized file. Dropper Malware executes fraudulent PowerShell and PowerShell scripts and downloads and executes a remote control malware from the attacker's server. This enables remote control from an external terminal.

⑤ Expanded breach to several domestic points in China by repeating ③ and ④.
⑥ Using method ②, the attacker intruded into the management server of anti-virus software in Japan from the terminal in China by remote control.
⑦ Like it did in China, the attacker expanded the intrusion into terminals at multiple points in Japan by repeating ③ and ④.
⑧ Likewise, it intruded into the server based in Japan using methods ③ and ④.
⑨ Externally transmitted confidential information on the server ⑧ via Terminal X.
⑩ The attacker received the confidential information via Terminal X.

The attacker who enters the internal network intrudes into other machines (④) by exploiting the distribution function (③) and vulnerability of the anti-virus software after intruding into the server (②) by abusing the vulnerability of the management server of the anti-virus software. The attacker expands the breach area by repeating ③ and ④.

The attacker uses at least lateral movement methods 1 and 4 in Table 3 in this case. It is considered that the attacker used these methods for the following reasons.

- As Mitsubishi Electric restricted functions of PsExec, WMI and PowerShell which could be abused for lateral movement, the attacker could not abuse them.
- As Mitsubishi Electric might have monitored behaviors of functions of PsExec, WMI and PowerShell which could be abused for lateral movement, the attacker used methods which were difficult to be detected.

In this way, this case is considered to have been an advanced cyber attack as the breach reached wider areas through lateral movement even in an internal system environment where it was assumed that measures for lateral movement methods used frequently by attackers had been taken.

2.2.2. Measures

What security measures should we take against such advanced attacks? There are various measures but we will introduce measures focusing on the end point where confidential information is stored, which is the target of attackers.

Prevention of lateral movement

Limit the movement of attackers between networks using an air gap or micro-segmentation and prevent them from reaching confidential information using lateral movement.

Air gap is to physically isolate a machine that stores important confidential information from the network, etc. connected to the Internet. It reduces the risk of attackers reaching a machine that stores confidential information and the risk of confidential information being stolen when they have intruded, as the network is not physically connected.

Micro-segmentation divide segments into smaller units compared to segments when network is designed by existing octet unit and limit data transmission between segments to a minimum volume. It can limit the area of attacker's movement when they have intruded and reduce the risk of expanding the damage. However, these two measures might have a significant impact on the operation and availability of information. It is recommended to apply these measures with modulations, such as to highly confidential information only and not all information, taking into account the confidentiality, availability and operation of information.

For unauthorized access to highly confidential information by advanced cyber attacks, it is better to take measures based on the following ideas.

- Handle information in an air-gapped environment where possible, taking into account the operation and availability of information.
- If the above method is difficult, carry out the following micro-segmentation.
  - Divide segments by department unit which handles the information.
  - Place servers and terminals which operate/manage the department in charge of the management of Active Directory and anti-virus software in divided segments.

Prevention of confidential information breach

Encrypting confidential information stops attackers from reading and using information without the encrypting key even if they could access the information.

To counter stealing of confidential information by advanced cyber attacks, it is better to take measures based on the following ideas.

- Encrypt confidential information using the algorithms listed in the E-Government Recommended Ciphers List.
- Appropriately manage the key used for encrypting so that attackers cannot access only with the identification information authentication of OS.

Attack detection and response at endpoints

If you introduce EDR (Endpoint Detection and Response) or analyze machine information using SIEM (Security Information and Event Management), you can detect behaviors of the attacker on client PCs and servers at an early period and post-detection responses would be carried out smoothly.

- By collecting information of a machine such as process and registry controls and analyzing it using EDR itself or SIEM, you can detect acts of attackers at an early stage including suspicious changes in registry (deactivation of network level authentication (NLA) in several Windows machines) and startups of many PowerShell processes more than usual in several Windows machines.
- Even if the breached machine is in a remote area, you can immediately investigate the breach status by displaying and analyzing the timeline of the processes using EDR or obtaining suspicious files.

- Even if the breach spread in a wide area and through many machines, you can immediately investigate the breach status by collecting information from several machines at the same time using EDR or searching processes, files and registries of several breached machines using Indicators of Compromise (IOC).
- You can respond remotely without going to the actual site to isolate the network of the breached machines and deleting suspicious files on the machines.

2.2.3. Conclusion

In the case of Mitsubishi Electric, defense-related companies were directly attacked. Government organizations, organizations related to defense-related companies and their clients can be targeted in some cases. These related organizations/companies could be targeted for advanced cyber attacks similar to Mitsubishi Electric. It is necessary to be careful of such supply chain attacks [29].

3. Data Breach

During the 1st quarter to the 3rd quarter of FY 2019, Web skimming data breaches were found continuously. The same trend was seen in the 4th quarter of FY 2019. In addition, many breach cases caused by setting errors in cloud services were reported, where anyone could browse information that is not supposed to be published to third parties on the Internet.

On the other hand, 2 data breach cases caused by setting errors in cloud services occurred in Japan. One of them was the Soft On Demand (SOD) case which became a big topic due to the breached contents.

3.1. Information leakage of SOD Prime - an adult video distribution service

SOD announced on March 19 that part of information of users who had a membership in their service “SOD Prime” was able to be seen from other users. The factor which caused the problem was the setting error set at the time of introducing CDN service for an access concentration measure. This incident leaked personal information of a maximum of 68,898 people to third parties and some information contained their name and video viewing history. As an apology, SOD paid 5,000 yen per person to users whose information including name might have been viewed and offered 500 points for the website for users who had information which might have been viewed.

3.2. Cause of leakage

In response to the spread of the novel coronavirus, on March 13, SOD started a free distribution campaign to offer part of their charged videos in their video distribution service “SOD Prime” without charge. After starting this campaign, access to the website greatly increased and SOD took a response measure to mitigate access concentration using CDN. However, there was an error in the setting when CDN was installed and when users accessed the service part, other user's personal information was displayed, which led to the leakage of personal information [30].

CDN is the abbreviation of Content Delivery Network and it is a system to efficiently deliver the same contents to many users in websites and video distribution services. In a normal website, a server which distributes contents is prepared in advance and when a large volume of access occurs the server load increases and causes a response drop or service stop. In order to solve this problem, CDN prepared a large volume of cache servers to temporarily store contents, which enables stable distribution for users who can obtain contents from the large volume of cache servers prepared.

Settings saved in the cache server of CDN were supposed to be those related to video contents only. However, as it required an urgent response, information including users' personal information was saved in the cache server by mistake in this case. In addition, there were repeated errors in the settings for CDN under this condition. When users tried to view their own information, information of other users saved in the cache server was displayed.

This is not the first case. Similar incidents occurred in Mercari [31] and the fan club website of the singer songwriter "aiko" [32], where part of other users' personal information was displayed in the same way. Therefore, SOD could have prevented the damage if it referred to these past incidents.

3.3. Impact of incidents

Looking at past personal data breach cases, a voucher of 500 yen was sent as an apology to victims of breach cases that occurred in Softbank BB and Benesse Corporation [33] [34]. In 2002, TBC experienced an incident where personal data including sensitive information such as body size and physical problems was breached. Victims of secondary damage brought a civil lawsuit and received a maximum of 35,000 yen consolation money [35].

For this incident, 5,000 yen per person was paid as an apology, which is higher than the amount paid for other personal data breach incidents, taking into account the significant mental distress from the disclosure of information which should not have been known by others including the viewing history of adult videos [30]. This incident revealed that organizations which handle information that might cause mental distress when breached need to take security measures more carefully.

Users also need to assume that such incidents might occur and make sure services they use take robust security measures before using them.

These are not all the impacts of such incidents. Breached companies need to pay great expenses for the investigation of incident causes, measures against re-occurrence, decrease in sales due to service stops and suppression of the brand image. The occurrence of such incident could lead to the rescission of security certification such as a privacy mark, although it did not apply this time [36]. Rescission of the certificate could have a significant impact on the business including a ban on bidding on transactions with a security certification requirement.

3.4. Conclusion

We focused on a data breach case related to setting errors in cloud services. At present, various cloud services are provided including CDN and it has become easy to expand services and volume. On the other hand, damage caused by setting errors tend to expand over a short period. In particular, when sensitive information is handled in a cloud service, we would like the service provide to provide services in a prompt and secure manner by referring to the best practice of the cloud service and efficiently checking setting errors.

4. Vulnerability

This Chapter explains the vulnerability (CVE-2019-19781) which arose in a product of Citrix. The Base value of the vulnerability published in JVN was 9.8, which is an extremely serious vulnerability. Organizations that have introduced the product are required to apply a patch immediately.

4.1. Vulnerability which arose in several products of Citrix.

On January 17, 2020, Citrix Systems announced that they confirmed attacks exploiting the vulnerability (CVE-2019-19781) which exists in Citrix ADC and Citrix Gateway (both Citrix products) which were released in December 2019. When this vulnerability was found, it was a zero-day vulnerability, which had no patches.

Normally, Citrix ADC and Citrix Gateway are network devices which allocate user requests to multiple servers. It has a user authentication and a single sign-on function for security [37]. When a user requests access to a file, the device process the request after judging whether the user who sent the request is a verified user and the user has an access right for the file. This time, a vulnerability of directory traversal has been found in the process of this pass. Attackers send requests by exploiting this vulnerability of the device on the Internet and read confidential data from system configuration files without user authentication.

On January 11, 2020, Project Zero India, a security researcher's group in India, published a proof of concept (PoC) code on GitHub, which can successfully attack exploiting the vulnerability [38].

SANS Institute, a security education company, reported that the number of scans (green line in **Figure 7**) targeted at this vulnerability in Honeypot increased after releasing PoC on January 11, 2020, which is shown as the wave line in **Figure 7**, and the number of exploit communications (red line in **Figure 7**) targeted at setting a backdoor by exploiting this vulnerability also increased after releasing PoC. As of January 11, security patches and a fixed version of the product haven’t been provided. The release of PoC has led to the occurrence of zero-day attacks. The fixed version was released on January 24, 13 days after the first exploit was detected.

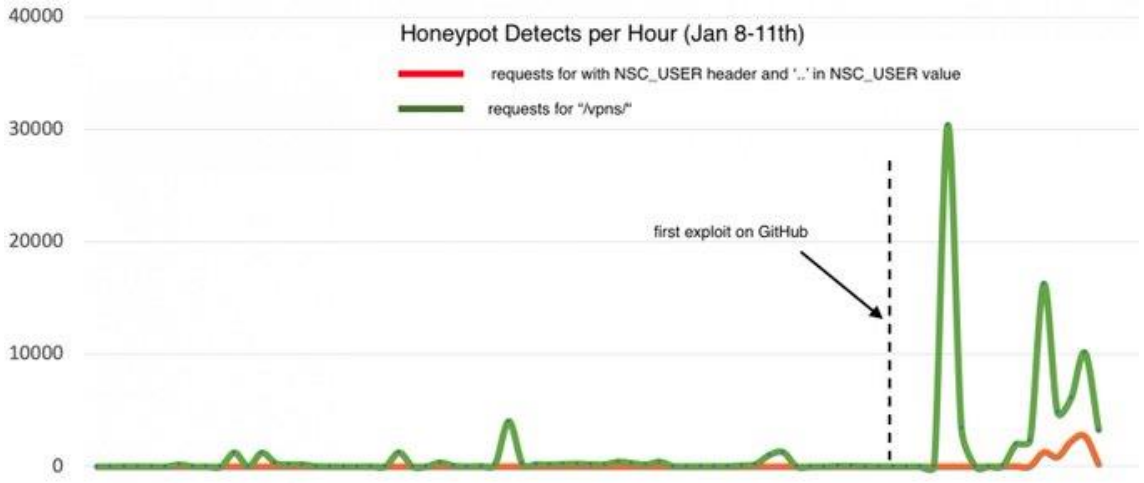


Figure 7: **Number of Honeypot Detects per Hour (Jan 8 - 11th)** [39]

4.2. Attack cases that use vulnerability of Citrix products

On January 20, Bretagne Télécom, a French telecommunications company reported that it was infected by ransomware DoppelPaymer which exploited the vulnerability of Citrix. As the Citrix product with fixed vulnerability was released on January 24, the attack to Bretagne Télécom was a zero-day attack.

Bretagne Télécom announced that the exploit encrypted 30 terabytes of data including data of about 30 clients and about 35 bit coins (equivalent to 350,000 dollars at that time) were demanded as ransom. As Bretagne Télécom had back-up data, all data was successfully recovered in 3 days, it did not have to pay the ransom money [40]. Bretagne Télécom could fortunately recover data. Was there any way to prevent the ransomware infection in advance? We do not know the cause of the vulnerability exploit of Citrix products from reports related to the Bretagne Télécom incident. In general, it might be one of the following 3 causes.

Vulnerability information of Citrix products was not recognized

Attacks cannot be prevented at all if the vulnerability information of Citrix products and warning of Citrix are not recognized. Measures are to always check the vulnerability information of Citrix products which is provided by the product manufacturer, distributors who signed a maintenance contract or a security agency. The free databases which can investigate vulnerability information are JVN in Japan, NVD in US and CNNVD in China.

Use of Citrix products could not be stopped

When Citrix Systems publish vulnerability in December 2019, it issued a warning of ceasing product operation or carrying out mitigation [41]. If the company had immediately ceased the operation of the Citrix product following Citrix's warning, it wouldn't have been exploited by the ransomware. However, if the company had ceased the use of the Citrix product, it could have had a significant impact on business operation. For this reason, Bretagne Télécom could not go ahead with ceasing to use the Citrix product and it is considered that the decision error led to the infection of ransomware.

Delay in implementing mitigation

If it could not stop using the Citrix product, it could have implemented temporary mitigation of attacks by changing settings. For products which might have a significant impact on the company's business operation, it is necessary to verify operation before changing any settings. As it took a long time for the company to verify the operation, attacks came earlier than the mitigation measure. If it takes a long time to implement mitigation measures and the mitigation cannot fully prevent attacks, it could have chosen a way to execute a remote code or detect ransomware infection early by temporarily strengthening monitoring.

4.3. Conclusion

We explained the vulnerability of Citrix products in this report. In 2017, there was a vulnerability exploit which spread the ransomware WannaCry throughout the world. In the case of the WannaCry infection, there was some time before large-scale attacks occurred from the release of vulnerability (CVE-2017-0144) in Windows Server Message Block (SMB) in March and the provision of fixes and patches. It is assumed that it was more difficult to deal with the vulnerability of Citrix products than that of the WannaCry case as it was a zero-day attack.

If the cause of ransomware infection was the misjudgment of Bretagne Télécom on system cease and setting changes, the factor was that it could not predict the exploit that could have occurred to the company from collected vulnerability information and decide appropriate responses. Using the vulnerability of Citrix products, the attackers could execute arbitrary code remotely and attacks started before the fixing patches were released. The security staff should have predicted the risk of great exploitation by attackers who might intrude into the company's network, and data breach and encryption by ransomware immediately after the vulnerability was released. If this was predicted, the company could have decided to cease Citrix product operation and set changes for emergency maintenance.

Security personnel of an organization should regularly check the vulnerability information of products which have a significant impact on the organization's business operation using the vulnerability information database listed above. If there are many types of products to

be checked, there would be a large amount of vulnerability information. Use tools to support the collection of vulnerability information of the products and information distribution services. Develop and use a method to evaluate the impact of vulnerability on business operation.

5. Malware/Ransomware

5.1. Summary of the 4th Quarter of FY 2019

As in the 3rd quarter of 2019, many exploitation incidents such as the malware Emotet and ransomware including Sodinokibi and Maze have been reported.

Emotet was found to spread via existing emails, but a new method of spreading the malware from infected terminals through Wi-Fi was also detected [42]. According to a report by Trend Micro, it is a subvariety of malware which exists since at least 2018. In Japan, Wi-Fi environments have been improved as a national policy [43] and there will be an increasing concern for exploitation in the future.

As for ransomware, the 3rd quarter report on information [44] said that some of the Sodinokibi and Maze types are found to steal information. During the 4th quarter, reports on victims who refused to pay a ransom payment and had their information exposed were prominent Previously, ransomware was in general a method to demand ransom in exchange for the availability of a system or organization by encrypting files on infected terminals. However, ransomware measures including backing up are spreading and due to the effect of promotion campaigns such as No More Ransom Project [45], it seems that obtaining ransom only by encrypting information is becoming difficult. Therefore, the amount of damage by data exposing ransomware attacks are likely to further increase in the future.

From mid February, 2020, many cases targeted at spreading malware using phishing methods have been reported, which were taking advantage of the global spread of the novel coronavirus. It is not uncommon for attackers to develop an attacking campaign taking advantage of public attention. However, according to an interview by Bleeping Computer, a computer help site, some ransomware attackers issued a statement that they “will not attack medical institutions [46].” Although it appears to be an official stance from a humanitarian viewpoint, it is expected that the suffering of global economy from long-term coronavirus damage is not a situation for ransomware attackers to be able to overlook.

5.2. Data exposing ransomware damage

In December 2019, Southwire (US) experienced damage from Maze ransomware. A report says that around 120GB of files were stolen by the ransomware from 878 devices [47]. After that, when the company refused to pay a ransom of about 6 million dollars, the attacker exposed about 12GB of files on the website the attacker operates..

Southwire was put in a predicament and decided to file a lawsuit. It was against an unknown attacker of the Maze ransomware. The court ordered suppressing of the website to the agent which was hosting the attacker's website and the agent followed the order. At one time, it looked as if they successfully stopped the data breach. However, the attacker showed an uncompromising attitude. The attacker disclosed 14GB of additional files and repeatedly threatened the company saying “if you do not pay ransom, we will publish more files.”

Southwire’s response was only a cat-and-mouse game with the attacker and it did not solve the problem. On the contrary, it may have egged on the ransomware attacker even more. Of course, this seems like a good opinion after the event and we cannot criticize Southwire’s response so easily. Once you are infected by data exposing ransomware, it is difficult to find a solution to the root cause. Even if the company had paid the ransom, there is no guarantee of the information being revealed. When you recognize an infection by data exposing ransomware, you should assume that data has already been breached. It is recommended that you try to take post-incident measures such as checking the scope of damage and immediately contacting related authorities and victims. Of course it is best to prevent infections. It is important to take inventory and evaluate the company's data assets regularly to prepare for prompt judgment in an emergency.

Table 4: Cases of data exposure by ransomware attackers

Date	Victim	Summary
2019/12	Southwire	Infection with the ransomware “Maze”. After refusing payment of ransom, some of the stolen data was published. Then the company filed a lawsuit against the ransomware attacker.
2019/12	Pensacola City, US	Infection with the ransomware “Maze”. There was a report that only a small portion of the data was actually stolen. With the aim of countering that report, some of the stolen data was published.
2020/1	Artech Information Systems	Infection with the ransomware “Sodinokibi”. 337MB data out of stolen internal data was published on a Russian hackers’ forum.
2020/1	MDLab	Infection with the ransomware “Maze”. After refusing payment of ransom, 9.5GB of stolen data was published.

2020/2	BretagneTélécom	Infection with the ransomware ”DoppelPaymer”. Payment of ransom was refused as it recovered data from backup files. After that, data of employees and digital certificates were exposed.
2020/3	Visser Precision	Infection with the ransomware ”DoppelPaymer”. After refusing payment of ransom, part of data related to defense and space development was published.

5.3. Conclusion

In Japan, the malware Emtoet went on a rampage. Damage from ransomware including Maze and Sodinokibi has been a big topic in the US. Previously, ransomware was targeted at local governments and medical institutions, and demanding ransom in exchange for recovering encrypted files was a major tactic. In the 4th quarter of 2019, however, there have been more data exposing ransomware attacks that were targeted at private companies, in which ransom is demanded in exchange for not exposing data stolen from an organization. Once information is stolen by data exposing ransomware, it is difficult to recover it. Therefore, it is recommended to assume that the stolen information has already been breached and try to take measures for restoration. Amid the spread of the new coronavirus, urgent economic measures and financial support systems for nation's citizens are rapidly being developed worldwide. There are quite a few attackers utilizing malware using new tactics by taking advantage of this panic. In Japan, JPCERT/CC and the Japan Cybercrime Control Center (JC3) are calling for attention as needed. Collect information on the latest cyber attacks and malware from these institutions and stay alert.

6. Outlook

Ransomware targeting individuals

In the 4th quarter of 2019, damage from data exposing ransomware which is targeted at private companies occurred frequently. As ransoms are refused to be paid in an increasing number of cases that use existing ransomware which encrypts files, data exposing ransomware can be main cause of damage in the future. It is expected that the scope of target will expand to individuals. It is common for individuals to own their own PCs and smart phones and devices owned by individuals are filled with personal data. In many cases, data which can cause social damage when it is exposed is saved. There may be ideal chances for attackers of data exposing ransomware if they target politicians and celebrities in particular.

Stay alert to attacks taking advantage of coronavirus

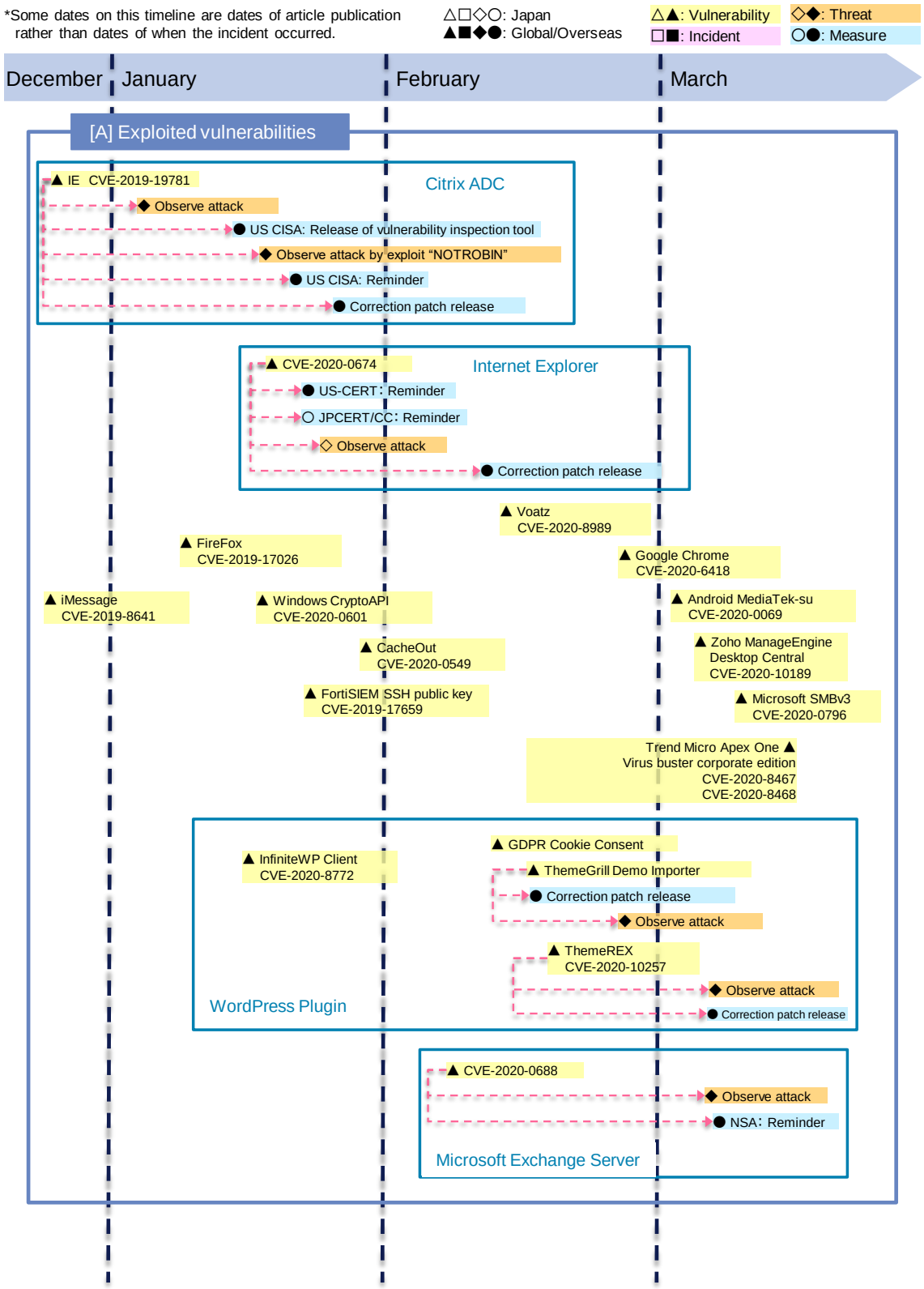
This document introduced coronavirus-related phishing attacks. According to a report of Proofpoint, more than 99% of cyber attacks require human involvement. Attackers take advantage of people's feelings of anxiety to carry out attacks and this situation increases the risk of successful cyber attacks. Coronavirus-related news are drawing the highest attention globally, and it is necessary to stay alert to phishing attacks. The Ministry of Health, Labour and Welfare of Japan has advocated a "New Lifestyle" and "thorough behavior modification [48]" and society is now on the verge of a significant change. It is likely that the chances of receiving phishing attacks will increase as communications depend on emails and SNS more than ever amid the coronavirus pandemic. If you sense something is suspicious, be sure to protect yourself against phishing attacks by seeking objective opinions of third parties rather than assessing the situation based on your own assumptions.

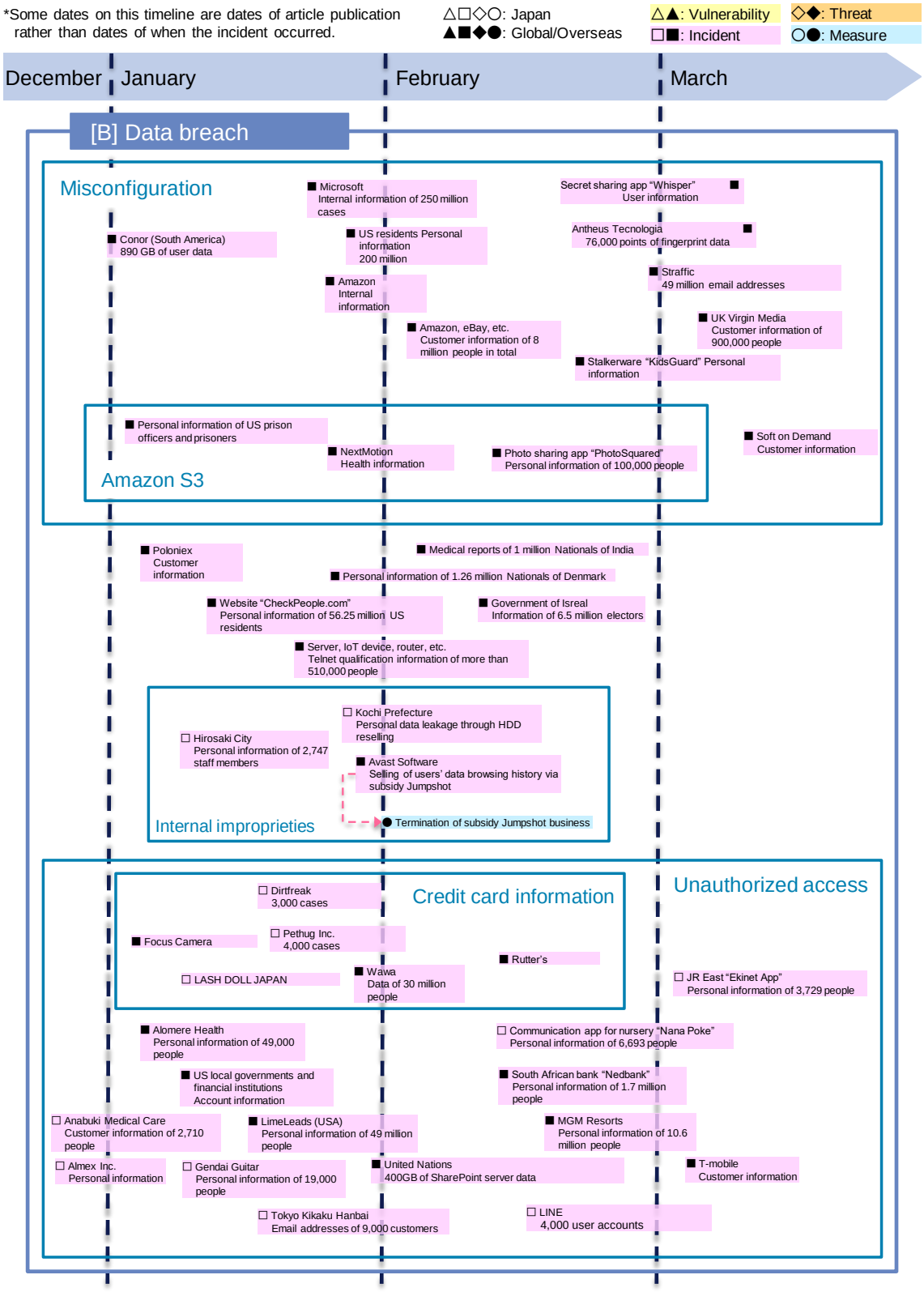
Increase in the number of supply chain attacks due to coronavirus

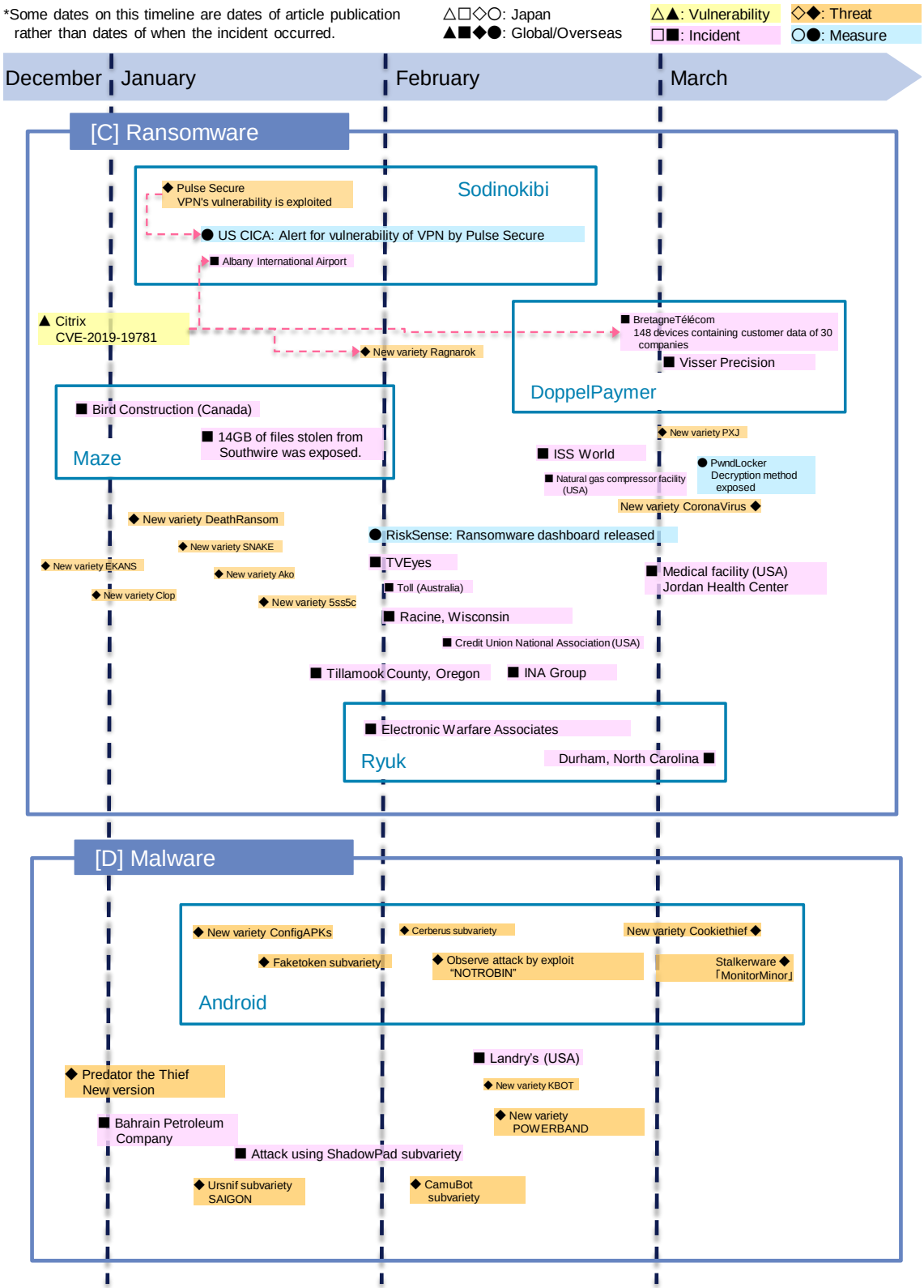
Decline in performance is a concern for many businesses affected by coronavirus. If business results decline, the budget for security will be reduced in the same way as other different budget reductions. The security level which an organization requires can become lower if the budget is reduced and the planned security measure is ceased or postponed, or the present security operation is downsized. On the other hand, attackers would strengthen attacks by taking advantage of this situation and increase the number of such coronavirus-related attacks that were introduced in this report [49] [50].

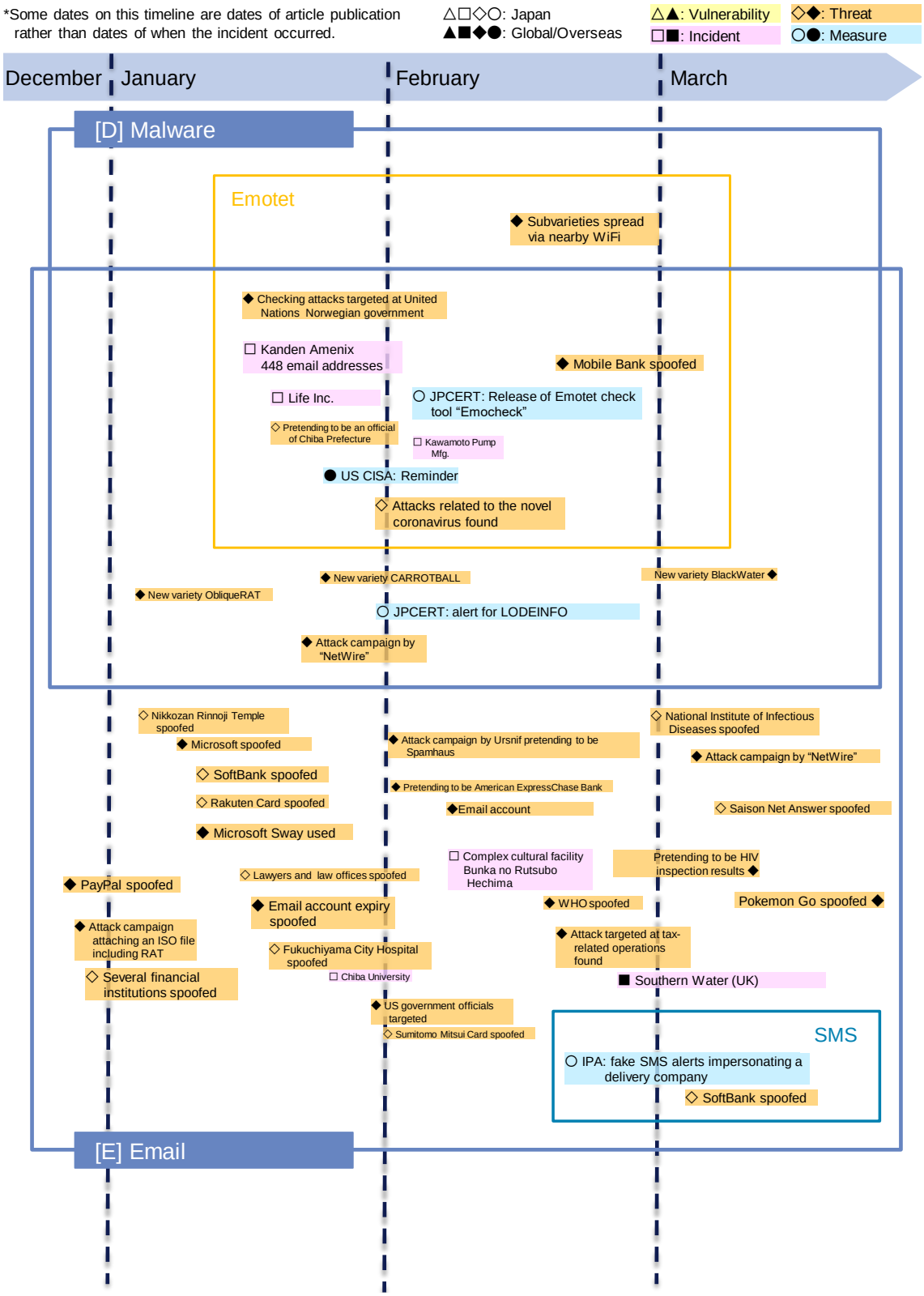
Taking the above situation into account, it is assumed that there will be more cyber attacks and damage. In particular, there is a risk of increased supply chain attacks which are targeted at points where advanced measures against cyber attacks haven't been taken. It is a harsh situation but attackers doesn't wait. It is recommended to compile a budget to secure the necessary security level and take measures.

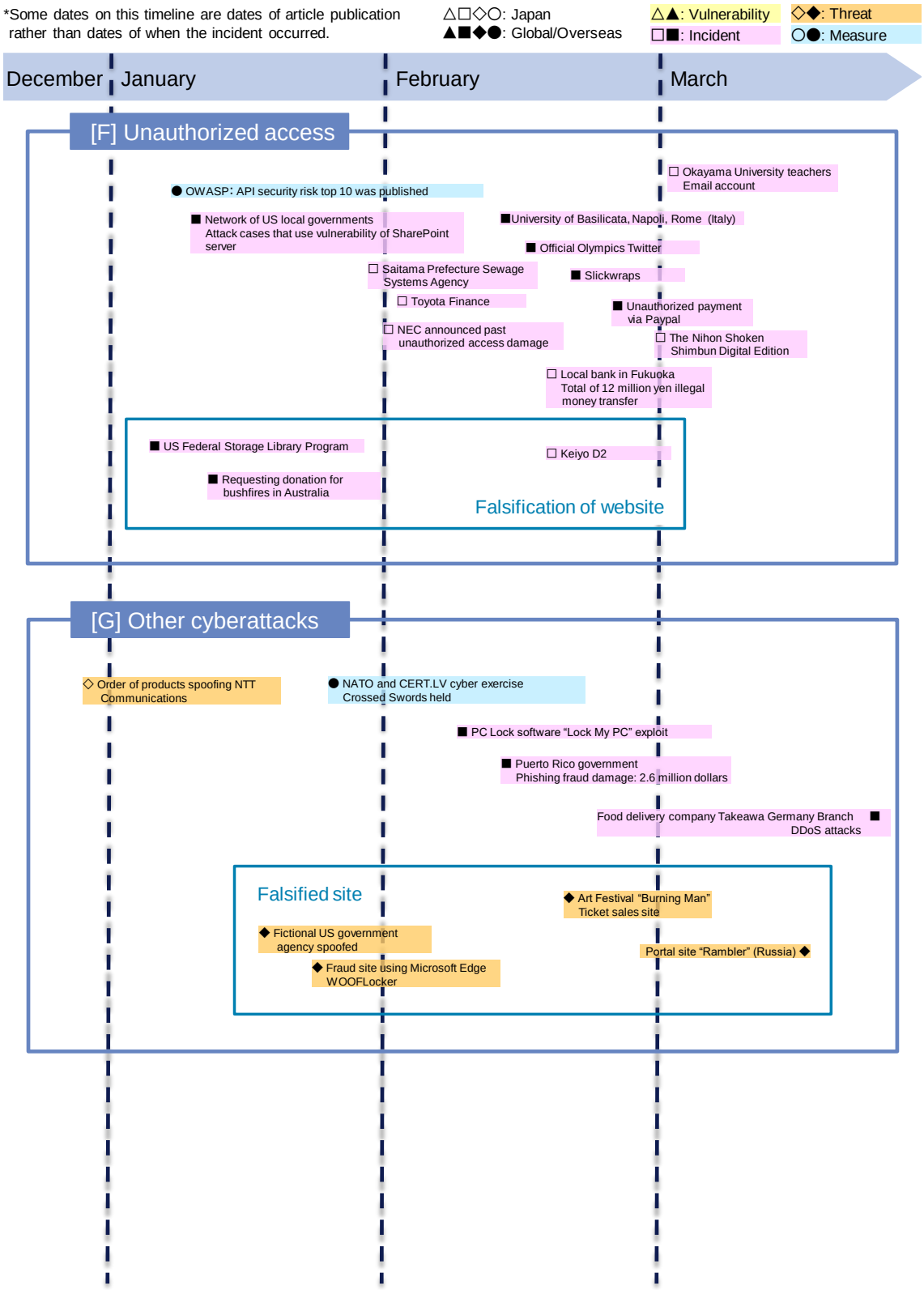
7. Timeline











8. References

[1] Check Point, “Coronavirus update: In the cyber world, the graph has yet to flatten - Check Point Software,” 2 4 2020. [オンライン]. Available: https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/.

[2] KnowBe4, “Q1 2020 KnowBe4 Finds Coronavirus-Related Phishing Email Attacks Up 600%,” 9 4 2020. [オンライン]. Available: https://www.knowbe4.com/press/q1-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-up-600.

[3] Reason, “COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report,” 9 3 2020. [オンライン]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/.

[4] So-net, “新型コロナ感染状況マップを装うマルウェアが登場,” 27 3 2020. [オンライン]. Available: https://securitynews.so-net.ne.jp/news/sec_30155.html.

[5] MITRE, “Azorult,” 26 7 2019. [オンライン]. Available: https://attack.mitre.org/software/S0344/.

[6] cyberreason, “Bitbucketを使用したマルウェア攻撃：正規プラットフォームの悪用,” 20 2 2020. [オンライン]. Available: https://www.cybereason.co.jp/blog/cyberattack/4381/.

[7] FORTINET, “偽の津波警報が日本にマルウェアを送り込む,” 28 12 2018. [オンライン]. Available: https://www.fortinet.co.jp/blog/threat-research/fake-tsunami-brings-malware-to-japan.html.

[8] Malware Guide, “Corona-Virus-Map.comを削除する方法,” 3 2020. [オンライン]. Available: https://malware-guide.com/jp/corona-virus-map-comを削除する方法.

[9] Lookout, “New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19,” 18 3 2020. [オンライン]. Available: https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19.

[10] DoaminTools, “CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware,” 13 3 2020. [オンライン]. Available: https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#.

[11] ESET, “2020年1月・2月 マルウェアレポート,” 31 3 2020. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2002.html.

[12] ikemen.tokyo, “[注意喚起] コロナウイルス対策としてマスク無料配布を語りAppleIDを要求するSMS,” 6 2 2020. [オンライン]. Available: https://ikemen.tokyo/2020/02/sms-musk/.

[13] 日本サイバー犯罪対策センター,“新型コロナウイルスに乗じた犯罪,”4 2 2020. [オンライン]. Available: https://www.jc3.or.jp/topics/newmodel_coronavirus.html.

[14] 佐川急便, “佐川急便を装った迷惑メールにご注意ください,” 14 5 2020. [オンライン]. Available: https://www2.sagawa-exp.co.jp/whatsnew/detail/721/.

[15] トレンドマイクロ, “実例で見るネットの危険：「新型コロナウイルス」に便乗する攻撃メール,” 4 2 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23740.

[16] kaspersky,“DNS設定を乗っ取りAndroidデバイスに感染するRoaming Mantis,” 17 4 2018. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis/20105/.

[17] kaspersky, “Roaming Mantis パート2：さらなる多言語化、フィッシング、そしてマイニング,” 18 5 2020. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-update/20383/.

[18] kaspersky, “Roaming Mantis パート3：iOSでの仮想通貨マイニングと、悪意あるコンテンツ配信システムを介した拡散,” 12 10 2018. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-new-methods/21749/.

[19] kaspersky, “Roaming Mantis パート4：Apple iOS向けの悪意ある構成プロファイル、アップデートされた悪意あるapkファイル（MoqHao/XLoader）の再拡散,” 4 4 2019. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-part-iv/22949/.

[20] kaspersky, “Roaming Mantis パート5：スミッシングによる拡散とリサーチャー避けテクニックの強化,” 8 2 2020. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-part-v/26912/.

[21] Security NEXT, “スマホ狙う「Roaming Mantis」、新型コロナ便乗も,” 2 3 2020. [オンライン]. Available: http://www.security-next.com/112732.

[22] Forbes, “世界で勃発の「コロナ給付金」詐欺、ドイツでは100億円の被害,” 26 4 2020. [オンライン]. Available: https://forbesjapan.com/articles/detail/34051.

[23] GlobalSign, “SSLの種類と利用用途,” 3 7 2019. [オンライン]. Available: https://jp.globalsign.com/ssl-pki-info/ssl_beginner/types-of-ssl.html.

[24] 三菱電機株式会社, “不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）,” 三菱電機株式会社, 12 2 2020. [オンライン]. Available: https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf. [アクセス日: 18 5 2020].

[25] 防衛省,“三菱電機㈱による機微な情報の漏えいの可能性について,” 10 2 2020. [オンライン]. Available: https://www.mod.go.jp/j/press/news/2020/02/10a.pdf.

[26] 三菱電機株式会社, “不正アクセスによる個人情報と企業機密の流出可能性について,” 20 1 2020. [オンライン]. Available: https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf.

[27] MITRE, “Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®,” MITRE, 19 7 2019. [オンライン]. Available: https://attack.mitre.org/tactics/TA0008/.

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

[29] 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 2019年度 第2四半期,” 29 11 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[30] ソフト・オン・デマンド株式会社, “弊社運営の「ＳＯＤプライム」における個人情報等流出に関するお詫び及びお知らせ,” 27 3 2020. [オンライン]. Available: https://www.sod.co.jp/apology/index.html?date=20200332.

[31] 株式会社メルカリ, “Web版のメルカリにおける個人情報流出に関するお詫びとご報告 ※6/23追記あり,” 23 6 2017. [オンライン]. Available: https://about.mercari.com/press/news/article/20170622_incident_report/.

[32] Security NEXT,“ファンクラブサイトで不具合 - 会員情報を誤表示,”10 1 2020. [オンライン]. Available: http://www.security-next.com/111366.

[33] ソフトバンク株式会社, “お客様情報流出問題に関する、現時点までの調査結果と今後の対策について,” 27 2 2004. [オンライン]. Available: https://www.softbank.jp/corp/group/sbb/news/press/2004/20040227_01/.

[34] 株式会社ベネッセコーポレーション, “事故の概要,” [オンライン]. Available: https://www.benesse.co.jp/customer/bcinfo/01.html.

[35] 日経XTECH, “〔78〕過去最高の賠償金となったTBCの情報流出,” 19 2 2007. [オンライン]. Available: https://xtech.nikkei.com/it/article/COLUMN/20070215/262166/.

[36] 日本経済新聞, “ベネッセの「プライバシーマーク」が取り消しに,” 26 11 2014. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO80153440W4A121C1000000/.

[37] C. Systems, “Citrix ADC (旧称NetScaler ADC),” Citrix Systems, [オンライン]. Available: https://www.citrix.com/ja-jp/products/citrix-adc/.

[38] P. Z. India, “Remote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway [CVE-2019-19781],” Project Zero India, 11 1 2020. [オンライン]. Available: https://github.com/projectzeroindia/CVE-2019-19781.

[39] J. Ullrich, “Citrix ADC Exploits are Public and Heavily Used. Attempts to Install Backdoor,” SANS Institute, 11 1 2020. [オンライン]. Available: https://isc.sans.edu/diary/25700.

[40] S. Gatlan, “DoppelPaymer Hacked Bretagne Télécom Using the Citrix ADC Flaw,” Bleeping Computer, 26 2 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/doppelpaymer-hacked-bretagne-t-l-com-using-the-citrix-adc-flaw/.

[41] C. Systems, “CVE-2019-19781：Citrix Application Delivery Controller、Citrix Gateway、Citrix SD-WAN WANOPアプライアンスで任意のコードが実行される脆弱性について,” Citrix Systems, 17 12 2019. [オンライン]. Available: https://support.citrix.com/article/CTX269194.

[42] トレンドマイクロ, “近隣Wi-Fiネットワークを侵害する「EMOTET」の活動を確認,” 8 2 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/24017.

[43] 総務省, “平成30年版 情報通信白書｜無料公衆無線LAN環境の整備促進,” 3 7 2018. [オンライン]. Available: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd266220.html.

[44] 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 2019年度第3四半期,” 28 2 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2020/022801/.

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

[46] Bleeping Computer, “Ransomware Gangs to Stop Attacking Health Orgs During Pandemic,” 18 3 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/.

[47] Bleeping Computer, “Maze Ransomware Publishes 14GB of Stolen Southwire Files,” 10 1 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/.

[48] 厚生労働省, “新型コロナウイルスを想定した「新しい生活様式」を公表しました（新型コロナウイルス感染症）,” 4 5 2020. [オンライン]. Available: https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000121431_newlifestyle.html.

[49] Check Point, “Increase in Remote Working and Coronavirus Related Threats Creating Perfect Storm of Security Challenges for Organizations, New Survey Finds,” 7 4 2020. [オンライン]. Available: https://www.checkpoint.com/press/2020/increase-in-remote-working-and-coronavirus-related-threats-creating-perfect-storm-of-security-challenges-for-organizations-new-survey-finds-2/#.

[50] VMware Carbon Black, “Modern Bank Heists 3.0 | VMware Carbon Black,” 5 2020. [オンライン]. Available: https://www.carbonblack.com/resource/modern-bank-heists-3-0/.

[51] ESRIジャパン, “ジョンズ・ホプキンス大学の新型コロナウイルス感染状況ダッシュボード作成の裏側,” 17 4 2020. [オンライン]. Available: https://blog.esrij.com/2020/04/17/post-35916/.

[52] サービス&セキュリティ, “急増するフィッシング被害　二要素認証突破の手口と対策,” 29 1 2020. [オンライン]. Available: https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10604.

[53] Proofpoint, “The Human Factor 2019,” 9 9 2019. [オンライン]. Available: https://www.proofpoint.com/jp/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more.

Published on Friday, June 12, 2020

NTT DATA Corporation
Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Ryo Hoshino / Nobuo Idezawa / Tomohiro Ito / Daisuke Miyazaki / Risa Shishido /
Kazuki Shimizu
nttdata-cert@kits.nttdata.co.jp