NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

1st Quarter of 2020

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.

Information security issues of Zoom

The use of online meeting tools (web meeting tools) is increasing as working styles change due to the spread of novel coronavirus (COVID-19). Zoom, out of many online meeting tools, drew attention with a rapid increase in the number of users over a short period. At the same time, however, several vulnerabilities, critical issues concerning privacy protection, defects in specification and configuration have emerged one after another, which is raising concern about its security. Risk measures have been taken against some vulnerabilities and specification issues by Zoom. However, threats like "Zoom-bombing" which cannot be avoided by users unless attention is paid still remain. This report summarizes raised issues concerning Zoom and points to be noted when using Zoom as a checklist, based on the guidelines issued by IPA.

Security risk of telework in the "new normal"

COVID-19 was prevalent in the world even in the 1st quarter (April - June, based on settlement in March) of 2020. The economy has been shifted to a "new normal" environment all over the world in order to respond to this situation. A big change in particular was a full-scale application of telework in working styles such as remote access from computers at home, expansion of use in collaboration tools and cloud services, and a change in communication methods.

In the wake of these changes, there is an increasing number of risks including the leak of confidential information from home computers, the spread of intrusion into company systems, leak of confidential information on cloud services used by individuals and the spread of incident damage caused by judgment errors of individuals.

In the new normal environment like this, each organization must consider that the existing security measures do not apply as they are, the organizational governance does not reach and it is necessary for individuals to make judgment on risks. An organization needs to recognize these new facts, carry out risk analysis in the new normal environment and review its security measures.

Vulnerability of Pulse Secure products

CVE-2019-11510 is a vulnerability of Pulse Secure products which was first announced in April 2019. US-CERT was still giving an alert on cyberattacks targeted at this vulnerability in April 2020, after 1 year of the announcement. The reason of the prolonged impact of this vulnerability is that when the vulnerability is exploited and authentication information is stolen before a patch is applied, damage will spread even after the patch is applied. If a vulnerability which might lead to stealing of such authentication information is found, it is necessary to apply a patch as well as check for the presence of intrusion and change the password if it is likely to have been intruded. It is also necessary to enhance authentication by introducing a multi-factor authentication in SSL-VPN products.

Outlook

It is expected that the new normal in working style including telework will continue in the future. It is considered that business communications which have previously been performed in person will change to methods using online tools including Zoom. When using online business communications, one needs to understand the risk of identity fraud and swindles and prepare a way of authenticating identity and information reliability.

About 9000 vulnerabilities were reported in the first half of 2020. The number is likely to reach a record high of 20,000 in 2020 and it is expected that the number of attacks targeted at vulnerabilities of VPN products used in telework will increase. In VPN products, the time between the publishing of a vulnerability and the occurrence of intrusion after a cyberattack tends to be shorter. Therefore, it is necessary to respond to vulnerabilities in a prompt and accurate manner more than ever.

In addition, it is estimated that the use of Docker will increase as the use of cloud services expand in telework. As the number of attacks targeted at Docker with insufficient security measures is likely to increase, it is recommended to scan Docker settings using the best practice of containers and take measures after clarifying setting rule violations and setting errors.

2. Featured Topics

2.1. Information security issues of Zoom

The spread of the novel coronavirus has significantly changed the working style of many business people around the world. The movement to promote telework (remote work), by which people work at a place other than the office has been accelerated rapidly and the use of various SaaS services to realize this has spread. We will focus on Zoom out of many other tools, which drew attention as an online meeting tool (web meeting tool) and consider its security measures and points to note when using it.

2.1.1. Rapid increase in the number of users and various issues found

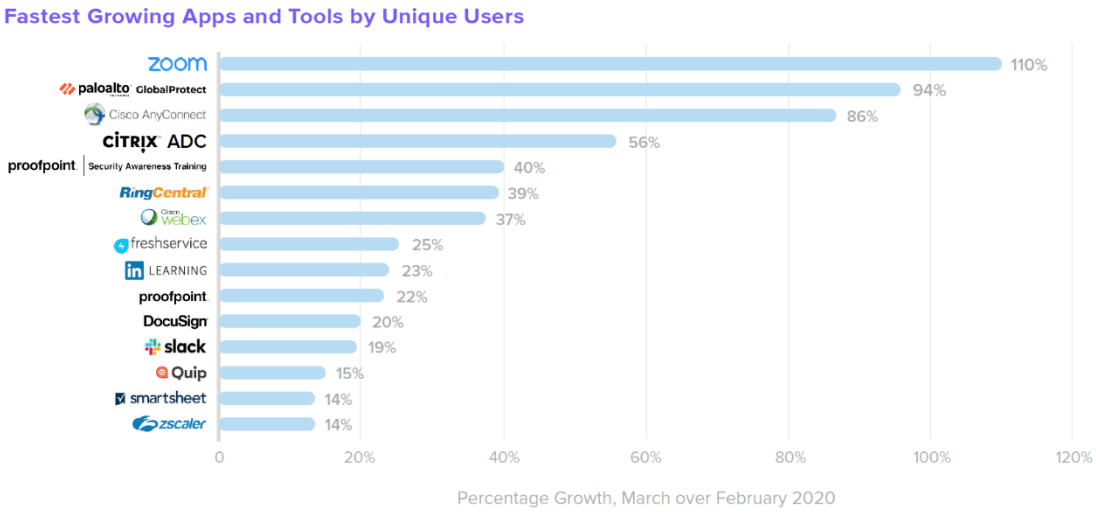


Figure 1: Growth rate in the number of SaaS tool users which were merged in Okta (Source: Okta website [1])

Figure 1 Shows the growth rate of login status to the SaaS tool which was merged in Okta, an IDaaS tool, between February and March 2020. It shows the number of Zoom users increased rapidly and it became the top service which realizes secure telework such as “GlobalProtect” of Paloalto and “AnyConnect” of Cisco. This trend is reflected in stock prices and the enterprise value of Zoom Video Communications (hereinafter referred to as Zoom), which created Zoom, is said to surpass that of a total of 7 large airline companies when compared on a market capitalization basis [2].

Although Zoom has many users as it is easy to use and stable, issues have arose one after another, such as several vulnerabilities being found, device analysis data being sent to Facebook without user's consent [3], and encryption of meetings was inappropriate [4], and concerns over security has spread. Some countries and companies have started restricting the use of Zoom.

2.1.2. Information security issues

When considering information security measures, there are three factors to be noted.

- [Confidentiality]: Only approved users can access information.
- [Integrity]: Information asset is accurate and not falsified.
- [Availability]: Users who have the right to access can access when needed.

In particular, [confidentiality] is the most important factor out of these three when using a web meeting tool. Web meetings are different from in-person meetings at an office in that participants access the meeting from their own environment. Therefore, there is a high risk of fraud, stealing and information leakage without realizing them. Below is the summary of issues which threaten [confidentiality] out of various security issues found in Zoom, including those released by Zoom.

(1) Vulnerability

Since the beginning of 2020, 8 vulnerabilities which were present in Zoom were released and have been registered in the vulnerability information database. Table 1 shows the summary of vulnerabilities and the level of impact which each vulnerability gives on confidentiality, integrity and availability. It shows that, out of 8 vulnerabilities, 6 have a “high” level of impact to confidentiality.

Table 1: Vulnerabilities of Zoom which are registered in CVE [5]

Common Vulnerabilities and Exposures	CVSS v3 base value*	Summary of vulnerability	Impact		
			Confidentiality	Integrity	Availability
CVE-2020-6109	9.8 Urgent	Vulnerability of path traversal. There is a possibility that writing on arbitrary files and arbitrary codes are performed from chat messages including animation GIF. [6]	High	High	High
CVE-2020-6110	8.8 Important	Vulnerability of path traversal	High	High	High
CVE-2020-11443	8.1 Important	Vulnerability concerning permission allocation	—	High	High

CVE-2020-11469	7.8 Important	Vulnerability concerning authority management	High	High	High
CVE-2020-11500	7.5 Important	Vulnerability concerning the use of cryptographic algorithm	High	—	—
CVE-2020-11876	7.5 Important	Vulnerability concerning the use of hard-coded authentication information	High	—	—
CVE-2020-11877	7.5 Important	Vulnerability concerning encryption strength	High	—	—
CVE-2020-11470	3.3 Warning	Vulnerability concerning the lack of authentication	Low	—	—

* Severity that is unique to vulnerability based on common vulnerability screening system (CVSS)

Other than this, vulnerabilities which are not registered in the vulnerability information database were also reported.

- Vulnerability of UNC path injection [7] [8]

Summary	The UNC path (a path to access folders and files on Windows network) which was sent to a chat window in a meeting is converted to a hyperlink in the same way as other URLs.
Issue	There is a risk of leaking credential information of users who click the UNC path sent by an attacker.

Vulnerabilities listed in the above (1) Vulnerability have already been fixed. When you use Zoom, make sure to update and use the latest version.

(2) Critical issues related to keeping the meeting confidentiality and user's privacy

Some critical issues are seen other than the vulnerabilities listed in the above (1) Vulnerability, such as encryption specifications which might cause users' misunderstanding and configuration fraud which might enhance the risk of privacy intrusion.

- It was found that end-to-end (E2E) of meetings has not been encrypted as defined. [4]

Summary	Encryption of Zoom meetings uses the encryption form in which "TCP connections use TLS and UDP connections are encrypted by AES using a key negotiated in TLS connections." It was found that the encryption form does not comply with the definition of E2E - "only users have the decryption key."
Issue	On the official website, Zoom explains that meetings use end-to-end encryption and this causes misunderstanding of users.
Response of Zoom	Zoom apologized about this matter [9], and installed E2E encryption, but the stock price has fallen drastically and shareholders filed a suit. [10]

- It was found that meetings go through a data center in China, where it is not supposed to be connected. [11]

Summary	A research team from the University of Toronto (Citizen Lab) had an actual online meeting using Zoom in order to investigate E2E encryption of Zoom. The team found out that the encryption key of the meeting was sent via a server in Beijing.
Issue	Based on the Cyber Security Law of the People's Republic of China, the Chinese base of Zoom requires acceptance of the request of information disclosure by the Chinese government and it is highly likely that confidential information of users is provided to the Chinese government.
Response of Zoom	Zoom pleaded that it has not mounted Geofencing (a mechanism which blocks communications to a specific area) on the application by mistake during the rapid process of development following the sharp increase in demand. [12]

- Terminal information was sent to Facebook without gaining user's consent. [3]

Summary	As Facebook SDK (software development kit) was used to login to Zoom with Facebook on iOS, terminal data including IP address and OS version (of users with or without a Facebook account) was forwarded to Facebook.
Issue	There was no statement that Zoom is sending data to Facebook for every startup in the privacy policy.
Response of Zoom	Zoom pleaded and apologized regarding this case and removed Facebook SDK [13] and updated its privacy policy [14]. However, it was filed a class action lawsuit for breaching the California Consumer Privacy Act as it was sending personal information to a third party without permission. [15]

- Vulnerability against wiretapping meeting details by users in the Waiting Room [16]

Summary	Zoom server automatically sends a decryption key of the meeting to all users in the Waiting Room.
Issue	Users in the Waiting Room might be able to wiretap details of the meeting without their participation being approved. A vulnerability was found although the key was introduced as a measure against Zoom Bombing written in the (3) Operational risk.
Response of Zoom	A measure was taken by fixing the program on the Zoom server.

(3) Operational risk

There is an issue which threats confidentiality depending on how users use Zoom, not an issue of the Zoom application itself.

- Zoom Bombing [17]

Summary	Attackers intruded into meetings after obtaining the meeting URLs which were shared via SNS, etc. There were many harassment cases reported, such as that attackers displayed violent images on the screen and used offensive language including hate speech. The FBI issued a warning on this case. Although it might be deemed simply as a nuisance, there is a concern about confidentiality when third parties who are primarily not relevant join the meeting.
Response of Zoom	Measures to prevent damage are published [9]

After issues had been found one ofter another, on April 1, 2020, Zoom announced that it will stop the development of new functions for a period of 90 days and will put resources into strengthening security and privacy [9]. At the same time, it appointed Alex Stamos, who worked as the CISO of Facebook, as an external advisor to try to improve the organization's transparency.

2.1.3. Organizations and companies which restricted or banned the use of Zoom

After a series of various issues were found, an increasing number of organizations and companies have banned or restricted the use of Zoom as a web meeting tool. Many said the reason of the restriction is “security concerns,” including no compliance with laws and company policies and suffering actual damage because of Zoom Bombing.

[Taiwan] It was recommended that government organizations not use Zoom [18]

- Taiwan has the Cyber Security Management Act which bans the use of tools that could bring concerns about data security. The country recommended government organizations and specific private organizations not to use Zoom as a series of security issues listed in the previous paragraph might “bring concerns about data security.”

[India] It was recommended that government officials not use Zoom [19]

- The number of Zoom application downloads for mobile terminals in India was the largest in the world in April [20]. The Ministry of Home Affairs recommended government officials not use Zoom because “Zoom is not a secure platform.” At the same time, the ministry released guidelines for individuals when using Zoom. At the beginning of May, there was an announcement that the country started the development of a domestic web meeting tool which would compete with Zoom. [21]

[Google] It announced that it will configure the settings on employees' PCs to disable Zoom. [22]

- Google announced that it will ban the use of Zoom on employees' PCs and configure the settings to disable the desktop version of Zoom, because the various vulnerabilities listed in the previous paragraph do not meet the security criteria set by the company.

Other than this, the New York City Department of Education and the Ministry of Education, Singapore will ban the use of Zoom to protect children's privacy and the same measure is taken in NASA and Australian Army which handle confidential information. This trend started after Zoom made an apology and it was reported that they fixed the vulnerability, which is probably the result of the judgment that the risk of using Zoom is very high for organizations which handle information requiring high confidentiality. It shows that it is not easy to recover credit once it is lost.

2.1.4. Points to note when using Zoom

Even if you use the latest version of Zoom in which vulnerabilities are fixed and an appropriate encryption system is installed, there still remains some risk which cannot be avoided unless users are careful, such as Zoom Bombing. We will summarize the points to note when using Zoom in a check list form based on the "Security precautions when using a web meeting service" [23] issued by IPA.

Table 2: Precautions by IPA and coping methods in Zoom

Precautions by IPA	Coping methods in Zoom
Whether the restrictions of meeting participants are clarified and appropriate configurations are set for the meeting.	☐ A passcode can be set for the meeting. ☐ By enabling the Waiting Room function, only participants approved by the host can join the meeting. ☐ When all participants are present, the host can lock the meeting room to block other users.
If a private meeting is held, set the meeting option to "private."	
In order to prevent uninvited participants from attending, set a meeting password and enable the Waiting Room function.	
Check the function for pre-approval when participants enter the meeting room.	☐ You can preset turning on/off[*1] participants' camera and microphone, screen sharing, enabling/disabling remote control for shared screen[*2] and enable/disabling private chats. *1 Turning off the camera and microphone is rather effective to prevent damage from Zoom Bombing. *2 It is desirable to turn off screen control by other users when not necessary to prevent the display of unintended information.

	Depending on the confidentiality of the meeting and the number of participants, use appropriate functions such as sending meeting information by email and a password via a separate route, two-factor authentication of participants, in-advance registration function for participants, etc.	☐ The passcode embedding can be omitted in a meeting link. *A passcode embedded link is highly functional in that participants can join the meeting with one click.
Whether the feature of forcing a participant to leave is available in case an unwanted participant joins the meeting.		☐ Host can force participants to leave a meeting. ☐ Host can configure their settings to allow removed participants to rejoin.
Whether a person in charge of checking participants is clarified to prevent uninvited third parties to join the meeting, especially in a meeting with participants outside the organization.		☐ Host can prevent uninvited participants to join a room by configuring settings not to allow participants to join before the host. ☐ Allowing participants to change their name enables them to participate with a name which can verify their identity.
If meeting data such as meeting recording, recorded data, shared materials, chat logs, etc. exist in the cloud storage, check if the data is moved to client terminals and is encrypted, and if it is removed from the cloud.		(Those with free membership can save recording/recorded data in local storage, and subscribed members can save data in the Zoom cloud storage as well as local storage.) ☐ Host can configure settings to remove records in the cloud. ☐ There is a setting to automatically remove records in the cloud on a defined date. ☐ There is a function to notify with a sound at startup/end recording in order to prevent unintended recording of sound and video by a third party. ☐ The function of sending a file in a chat can be turned on/off in advance. *Sharing files in a chat generates a potential risk that uninvited participants can send a suspicious file which spreads malware.

Other than this, when using not only Zoom but all tools, it is necessary to check if the application used is the latest version and if the virus definition files on the terminal are up to date. It is not recommended to share a meeting link and password for business on SNS. If the meeting is highly confidential, it is better to use an email subject which confidentiality cannot be guessed and send the password via a separate route.

It is not possible to determine uniform criteria to use or not to use Zoom in company meetings as we need to consider the type and confidentiality level of meetings and characteristics of the industry. It is important to determine clear policy and rules for each organization and use the application in a way that complies with them. We suggest you review how you think of Zoom in your own environment and how you handle it by referring to this article.

2.2. Security risk of telework in the “new normal”

COVID-19 was prevalent around the world even in the 1st quarter of 2020. Coronavirus-related cyberattacks have also continued to occur in cyberspace.

Figure 2 is a graph showing changes in the number of coronavirus-related cyberattacks which were identified by a solution of Check Point between January and June 2020, which was released by the company. In late April, about 4 times more coronavirus-related attacks than those at the end of March occurred. After that, the number of attacks has been on a decreasing trend but the number in June was about 2.5 times more than that at the end of March. The number of coronavirus-related cyberattacks during the 1st quarter of 2020 was much larger than that during the 4th quarter of 2019 when these attacks started appearing. Coronavirus-related attacks have also occurred in Japan.

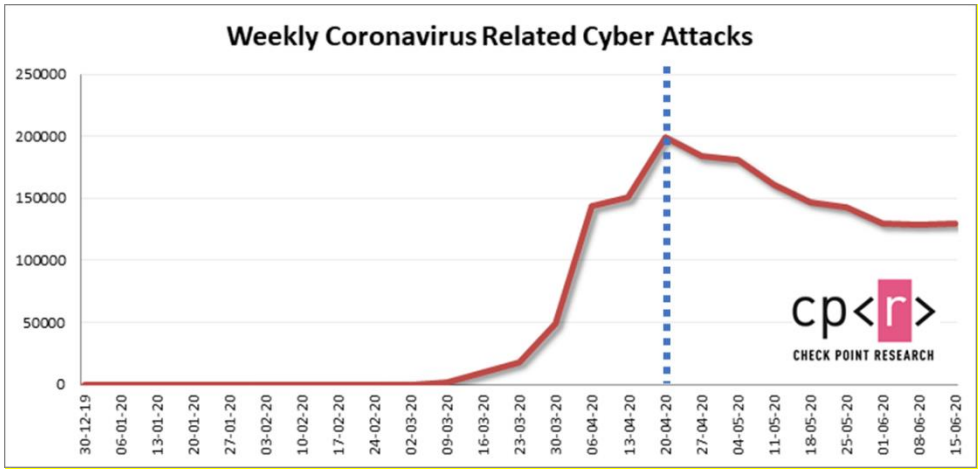


Figure 2: Changes in the number of cyberattacks related to coronavirus (Source: Check Point Blog [24])

From around May 2020, Japan started to introduce “New Lifestyle” which is different from the previous lifestyle to address the situation concerning COVID-19. In the same way, the whole world has shifted to the new normal lifestyle to live together with COVID-19. The most significant of such changes was working style which changed to telework: working time makes up a large percentage of one’s life, it affects many people because not only workers but those related to them are affected, and changes in business location, operation, system, etc. If working environment, technology and operation change significantly, many cases which cannot be covered by existing security measures occur. Attackers target this change in working style to telework to carry out new cyberattacks.

2.2.1. Attack cases targeting telework

In Japan, the use of telework, flex time and infection control measures started in offices between April and June 2020, when a State of Emergency and other measures were declared. The percentage of teleworkers increased from 31% in mid March to 62% in early April in the US [25]. Likewise, working environment has changed significantly in various countries. We will introduce 3 attacks which increased in response to this change in working environment.

The first is Brute Force Attack which attacks devices that can connect by remote desktop protocol (RDP). RDP is a service necessary for telework. However, some people use it without adequate security measures to directly access the RDP port from the Internet. Between January and April, 2020 when the shift to telework just started due to the coronavirus pandemic, the number of RDP ports which could access via the Internet was about 3 million to 4.5 million, an increase by a factor of 1.5 [26] [27] [28]. The number of Brute Force Attacks to these RDPs has been increasing since March [29] [30].

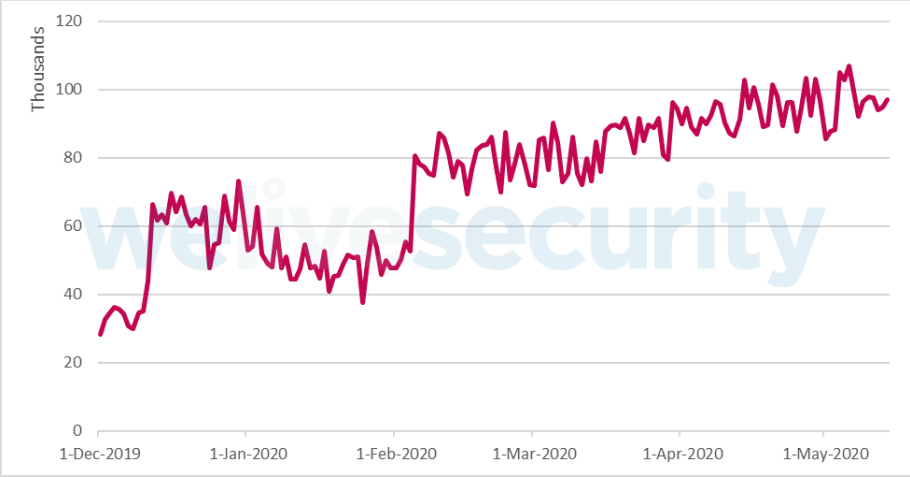


Figure 3: Trends of trial attacks to RDP against a single client (Source: ESET blog [30])

The second is phishing attacks targeting telework. The use of VPN connections, online meeting tools and cloud services has increased as the use of telework expanded. The number of phishing attacks increased by targeting these. The current methods of phishing attacks have not been changed much from existing methods, which sends phishing emails to lead users to a phishing site that steals authentication information. Below are phishing attack cases targeting telework, which emerged under the coronavirus pandemic.

Table 3: Phishing attack cases targeting telework [31] [32] [33] [34]

Phishing email contents	Phishing sites	Authentication information to be stolen
Notification to change VPN settings	Log in page of Office365	Office365
Notification on Zoom meeting	Log in page of Zoom	Company email address
Notification on chat conversations on Microsoft Teams	Log in page of Office365	Office365
Error notification on Webex certificate	Log in page of Webex	Webex

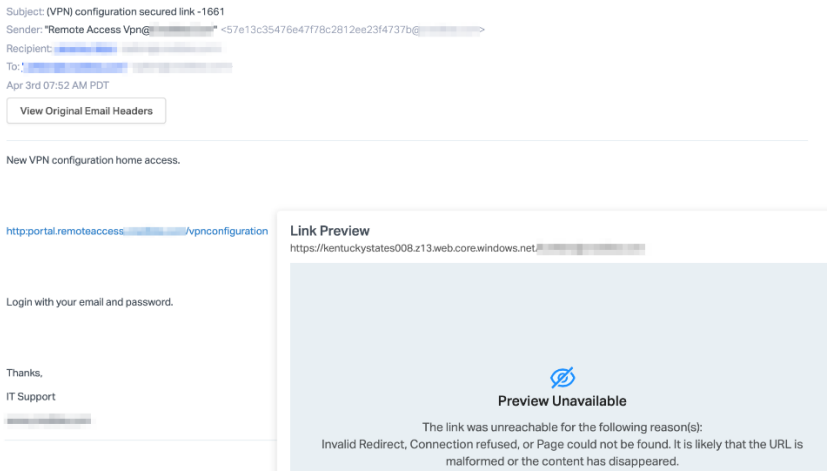


Figure 4: Phishing emails pretending to be a notification to change VPN settings
(Source: Abnormal Security website [31])

The third attack is the distribution of false installers and false smart phone applications targeting telework. Below are examples of false installers and false smart phone applications distributed by assuming Zoom, which had sudden growth in the number of users as an online meeting tool, and a VPN client software.

Figure 4: Cases of false installers/false smart phone applications targeting telework [35] [36]

False application	Target OS	Actions of false application at the time of installation
False installer of Zoom(1)	Windows	● A false installer force quit processes related to all running Remote Utilities. ● Add a setting to allow receiving of TCP 5650 port to Windows Firewall. ● Add a setting to send the following run state, etc. of the false application and a notification to the C&C server. ✓ Information of email recipients ✓ Already stole authentication information. ✓ Settings to notify that the infected PC is accessible to remote control server (C&C server) ● False installer downloads and installs genuine Zoom.
False installer of Zoom(2)	Windows	● The false installer downloads and installs malware which has the following functions and genuine Zoom. ✓ Obtains the screenshots of user's desktop and active windows. ✓ Scans the system and searches any connected web cam. ✓ Sends the above information to the C&C server. ● False installer downloads and installs genuine Zoom. ● After starting up the PC, automatically starts malware and sends all the collected information to the C&C server every 30 seconds.
False smart phone application of VPN client software.	iOS	● Downloads and installs a paid application from the App Store (passes the screening as there are no malicious actions such as stealing personal information from the device). ● There is a payment for subscription fee when downloading from the App Store. ● Cannot perform VPN connection even if the false smart phone application is started as it is not equipped with a VPN connection feature.

The methods of attacks used in any cases introduced above have not been changed much from existing cases. However, attackers make their attacks more successful by skillfully using the following new normal situation.

- Setting reviews and configurations are inadequate as the companies developed a telework environment in a rush with a focus on continuing operation.
- In a situation where people are not used to using VPN connections, online meeting tools and cloud services and the number of emails receiving is increasing, it is difficult to judge whether or not received emails are phishing attacks.
- It is easy to falsify things using false installers and false smart phone applications as there are many new users of the software.
- Correct information on new software for phishing attacks, false installers and false smart phone applications cannot be obtained nearby due to telework and it is difficult for users to consult supervisors and colleagues.

2.2.2. Risk of telework in the new normal

The aforementioned attack cases targeting telework are just a part of all attacks. The risks of the following changes caused from telework are analyzed to see what types of security risks there are other than the above.

(1) Remote access from home PC
(2) Expanding use of collaboration tools
(3) Expanding use of cloud services
(4) Changes in communication methods

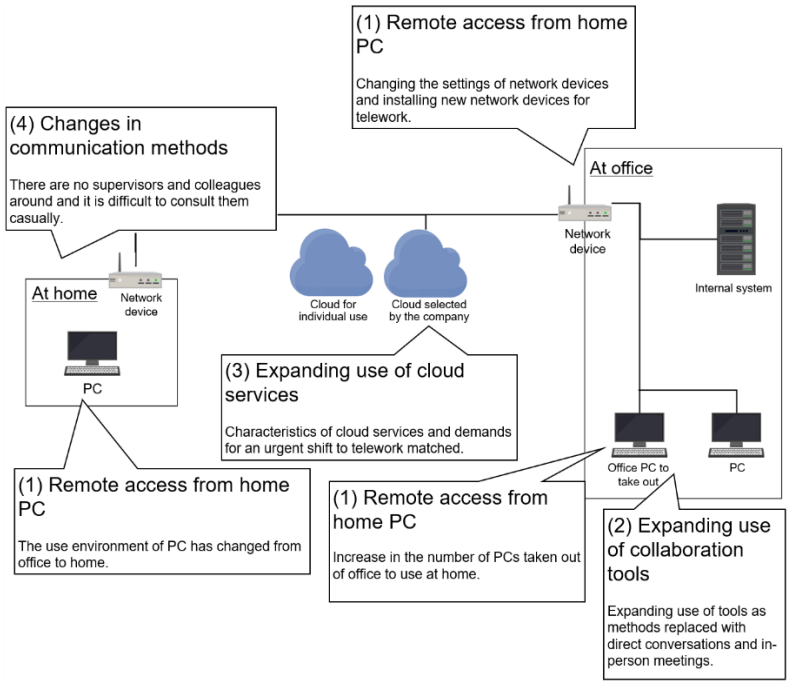


Figure 5: Changes caused from telework

(1) Remote access from home PC

The first is the risk of cyberattacks to a PC itself and the damage caused from bringing the PC home and changing the environment of PC use from the company network to home network in order to handle telework. It is easier for various information security incidents (virus infection, ransomware damage, information leak, cryptomining, etc.) to affect PCs when they are not connected to a company network. PCs used for teleworking in particular have a higher risk of confidential information leak than those used in a company network, and it is expected that the number of information leak incidents will increase. Risks not only from confidential information leaks but authentication information leaks require attention when considering information leaks from PCs. If various authentication information leaks from PCs, it might develop into significant damage including a risk of BEC and intrusion into the company network and cloud environment. This is because the responsibility of applying security patches on the PC and security measures such as anti-virus were taken by individuals. Security measures have weakened as it is difficult to control the automatic application of security patches on PCs in the same way as they are connected to a company network.

The second is the risk that attackers intrude into the company network and cloud, and malware gets into the company network and machines. Incidents such as bringing malware via PCs taken out of a company or attackers intruded in the company network via the backdoor on PCs have occurred even before telework spread. However, the number of PCs taken out of company offices is significantly increasing following the spread of telework and the number of the above risks is increasing. The factor of these risks is that the existing security measures based on the idea of border protection is not adequate measures against risks in the telework-based working environment. We need to consider and carry out security measures based on the idea of Zero Trust.

The third is the risks caused because settings of network devices were changed and new network devices were introduced in haste in order to correspond with telework. The above risks are caused because network devices were introduced in haste with a focus on usability to continue business operations. Reviews of setting changes and secure configurations were probably not sufficient in network devices. In addition, attackers are focusing on targeting the vulnerabilities in network devices for rapidly expanded telework, which is another factor.

(2) Expanding use of collaboration tools

It has become difficult to have opportunities to talk or hold meetings in person due to telework. To supplement this, the use of communication support tools such as Microsoft Teams, Slack, etc. and online meeting tools such as Zoom, Webex, etc. has expanded. In accordance with the use of these tools, new risks have emerged. These tools have file sharing and chat features and a function that allows various people to join the meeting online. There is a risk of confidential information leaks related to business when attackers try to make bad use of these tools or when users perform wrong operations. For example, an attacker requests

to join a chat by pretending to be a related person and if the user accepts it by mistake, chat contents and files shared in the chat will leak.

(3) Expanding use of cloud services

The use of cloud services has been expanding following the spread of digital transformation. The use of cloud services has expanded further to correspond with the use of telework. We will pick up two major risks in using cloud services when teleworking.

The first risk is the risk concerning cloud services used in an organization. Incidents like information leak have occurred in cloud services before the new normal because: compared with on-premises environment, anyone can develop a cloud environment easily without considering security measures and as the method of security settings is significantly different, setting defects are easily generated. In addition to the above, security configurations of the cloud might be insufficient as the use of cloud services started in a short period prioritizing the operational continuity to correspond with the rapid shift to telework. If you have started to use a cloud service in a short period, it is recommended to review settings immediately. If your skills are not sufficient to review, it is useful to use a cloud security posture management (CSPM) product which automatically detects setting defects, etc. and a diagnostic service of settings, etc.

The second is the risk concerning cloud services used by individuals. As it is difficult to control cloud services used by individuals working in a telework environment, it is easy for users to use a cloud service with a dangerous setting. If such cloud service is used in business, there is a risk of confidential information leak on a cloud service caused from an attack by a third party.

(4) Changes in communication methods

Unlike working in an office, there are no supervisors and colleagues around in a telework environment. Under this situation, one cannot casually consult someone on security issues when they do not know what to do if their PC might be infected by a virus or if they have received a phishing mail. In such cases, it is necessary to decide and act by yourself. However, damage might worsen when the decision is late or wrong and the response to incidents is delayed. This risk widely affects security measures under the new normal. As the working environment and communication styles changed dramatically, know-how of security management measures which have been accumulated so far will not work. We need to change the idea of security measures considerably without clinging to the existing common knowledge and experience.

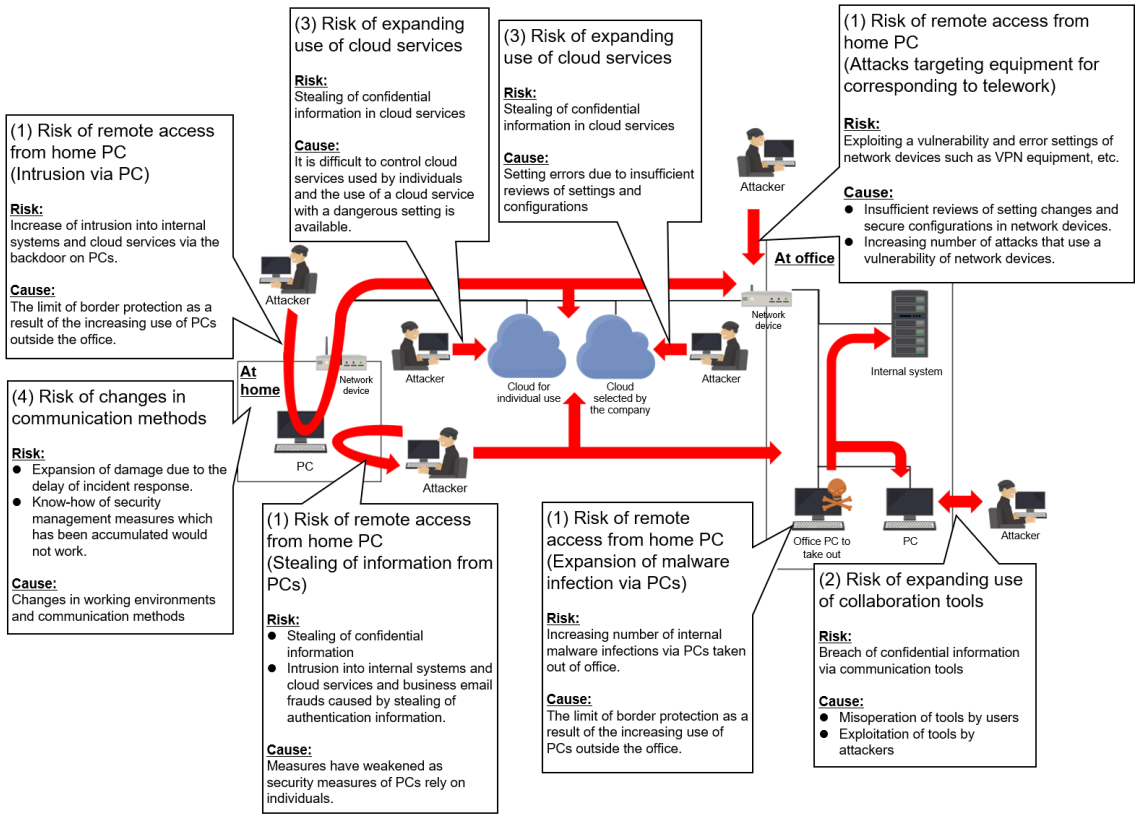


Figure 6: Risks associated with changes in telework

2.2.3. Conclusion

Many companies experienced great changes in the working environment due to the reform of working style which corresponds to the new normal including the shift to telework. Security risks have also changed significantly and new risks which were mentioned in the previous paragraph have emerged. It is unable to respond to security risks which changed dramatically with the existing security measures. Therefore, we consider it necessary to review security measures by implementing risk analysis in the new normal environment. It is recommended to take notice of the following points when implementing risk analysis and security measures.

- Risk analysis should cover not only a company's internal environment but cloud services and home environment used for telework.
- Existing security measures cannot be applied as they are.
- When considering a management plan for security measures, consider that a company governance would not reach cloud services, individuals' home, personal PCs, etc.
- Each individual needs to judge security risks. Technical security measures should be increased so as not to depend on individual's judgment.
- Make it easy for individuals to receive security-relate information. Prepare for a contact or method where individuals can consult someone casually.
- Consider response methods taking into account a case in which identification of the incident and response are delayed.

3. Data Breach

During the 1st quarter of FY 2020, data breaches from Web skimming and setting defects have been found consecutively since FY 2019. The Soft On Demand case attracted attention in the 4th Quarter of FY 2019. In the 1st quarter of FY 2020, information disclosure from a similar overseas adult video website was detected.

3.1. Information Disclosure of “CAM4”

It was found that 7TB of data totaling 10 billion and 88 million cases including personal information such as name, sexual orientation and payment records of users and internal information such as impropriety and spam detection log, etc. had been disclosed in the US adult video live chat platform “CAM4.” Safety Detectives, a security investigation group, conducted an investigation of disclosure service using SHODAN, a search engine for Internet connection devices, and identified this fact. When Safety Detectives contacted the Irish company Granity Entertainment which owns CAM4 about the information disclosure, it stopped disclosing information within 30 minutes [37].

3.2. Cause of Information Disclosure

The cause of the information disclosure was the setting error of the search engine ElasticSearch. Information which should originally be handled as confidential information was put in a state which can be viewed from outside due to a setting error. ElasticSearch is an open source full text search engine which can be used for application searches, log analysis, container monitoring, etc. It is used widely for on-premises environments and clouds. At present, it is unclear what setting error specifically caused the information disclosure. The past two information breach cases due to setting errors in ElasticSearch were both caused by a defect of login authentication. The cause of the CAM4 information disclosure might also have been a setting error in login authentication.

3.2.1. Similar case: Ecuador

On September 16, 2019, a VPN monitoring service company in Israel “vpnMentor” announced that information of almost everyone in Ecuador was available to view on the Internet. The information which could be viewed included personal information of a total of more than 20 million people such as name, date of birth, phone number, National lD number, family tree information, etc. The cause was that ElasticSearch was accessible without authentication. [38]

3.2.2. Similar case: Honda Motor Co., Ltd.

On July 31, 2019, Justin Paine of Cloudflare found that email addresses of Honda Motor's employees and security-related information in the internal network was available to view. In particular, security-related information included a vulnerability in security measures, application patches and end point security software status.

The cause was that ElasticSearch was accessible without authentication. When Honda Motor checked access logs, there was no sign of a third party downloading data [39].

3.3. Response to CAM4 and data breach prevention measures

According to an investigation by Safety Detectives, it was announced that ElasticSearch of CAM4 did not have any sign of a vicious third party's access and no data breach was detected. After being contacted by Safety Detectives, the company acted promptly to stop the access to information within 30 minutes, which prevented damage [37]. However, if the period of CAM4 log record is shorter than the period of information disclosure, the trace of access might have been deleted. If this was the case, personal information such as name, sexual orientation and payment records of users might have leaked.

It is effective to use a method to prevent setting errors by developing a setting procedure manual and a method to investigate accessible communication ports by carrying out regular network scan of services used on the Internet side. This is because it is desirable to configure settings not to disclose the administrator login page of ElasticSearch to the outside. In addition, in order to detect cyberattacks and information breach from vulnerabilities in an early stage, it is effective to install a tool to monitor access to ElasticSearch from the outside and regularly investigate logs.

3.4. Conclusion

Although more than 10 billion records were available to view from the information disclosure of CAM4, data leakage was not found and a serious situation was avoided. However, one single misstep could have caused a large information breach accident. The development of the cloud allowed people to easily develop a service and publish it on the Internet. On the other hand, developing a service and changing settings on the cloud without understanding the importance of security measures such as login authentication and access control are causing an increasing number of incidents. It is strongly recommended that when you develop a publishing service on the Internet using the cloud, do it based on the idea of basic security measures.

3.5. Information breach cases in the 1st quarter of 2020

Table 5: Information breach detected in the 1st quarter of 2020

Date	Organization	Cause	Summary
4/10	Fueru Mall	System vulnerability	Customer information of a maximum of 120,000 cases including 94 pieces of credit card information leaked due to SQL injection. [40]
5/7	NTT Communications	Cyberattacks	The server in the Singapore branch was attacked and it was likely that information of 621 clients leaked. [41]
5/8	The Nihon Keizai Shimbun	Phishing attacks	Infected with malware through an email attached file About 12,000 pieces of employees' information leaked [42]
5/19	Mercedes-Benz	Misconfiguration	Component for smart cars was disclosed on GitLab. [43]
5/19	easyJet	Cyberattacks	Customer information of about 9 million cases leaked by a cyberattack. [44]
6/9	Nintendo	Password list attacks	About 300,000 personal accounts used for purchasing game software leaked. [45]

4. Vulnerability

This Chapter explains the vulnerability (CVE-2019-11510) which arose in a product of Pulse Secure. If the vulnerability is exploited before the patch is applied, damage might spread even after patch application. It is therefore necessary to check the presence of intrusion and strengthen authentication.

4.1. Vulnerability which arose in products of Pulse Secure.

CVE-2019-11510 is the vulnerability of SSL-VPN products by Pulse Secure. By exploiting this vulnerability, attackers can avoid authentication and view any file.

As written in the Quarterly Report on Global Security Trends (the 2nd quarter of 2019) [46], this vulnerability was released in April 2019 and the patch has been published. However, attack cases that exploited this vulnerability have been reported after 2020. Under such situation, on April 16, 2020, US-CERT (CISA) issued a reminder (AA20-107A) [47] which summarizes exploitation cases and measures.

Table 6: News on CVE-2019-11510

Date	Summary
2019/04	CVE-2019-11510 was published [48] Pulse Secure released the patch
2019/08	Bad Packets observed scanning to try exploiting [49]
2019/09	JPCERT/CC issued a reminder Reminder about the vulnerability of several SSL VPN products [50]
2020/01	US-CERT issued a reminder (AA20-010A) [51]
2020/04	US-CERT issued a reminder (AA20-107A) [47]

4.2. Attack cases targeting vulnerabilities and countermeasures

Attackers can avoid authentication and view any files by sending a request with a URL incorporating a string which tries to attack the directory traversal. If the attacker successfully stole the authentication information of plain text by exploiting this vulnerability CVE-2019-11510, the attacker pretends to be a genuine user and SSL-VPN connection is enabled. Once the authentication information is stolen, the attacker can illegally access SSL-VPN connection after the patch is applied and the vulnerability is fixed. In fact, a case [52]was reported where an attacker illegally logged into a machine on the internal network using an SSL-VPN connection by exploiting authentication information after the patch was applied, and disabled end point security and installed ransomware.

If an SSL-VPN product of Pulse Secure which hasn't fixed the CVE-2019-11510 vulnerability is used, it is necessary to apply the patch first. As well as patch application, it is also necessary to investigate if there was an exploitation of vulnerability by an attacker before the patch was applied. However, any signs which show authentication information was viewed by an attacker exploiting a vulnerability were not found from the log. Therefore, it is necessary to check if there is any illegal access by exploiting stolen authentication information in the authentication log.

When checking stolen authentication information, check the trace of suspicious logins of an attacker who pretended to be a genuine user from the log. For example, check if there is different information from the user's normal state: host name, IP address, successful authentication in a different time and successful authentication in a short time with a big difference in the range of sender's IP address.

If it is likely that a vulnerability was exploited, make sure to change password of the administrator’s account to log in the Pulse Secure product and of all users’ accounts to connect to the Pulse Secure product through SSL-VPN.

4.3. Conclusion

We picked up the vulnerability of Pulse Secure products this time. Normally, a prompt patch application is important to respond to a vulnerability. It is however necessary to check if there is an intrusion before patch application for CVE-2019-11510, as the damage might spread even after patch application. If it is likely to have been intruded, measures including changing authentication information need to be taken.

According to an investigation by JPCERT/CC [53], there were 298 vulnerable Pulse Secure products in Japan as of March 24, 2020 and measures remain necessary. Due to the spread of the novel coronavirus and the expanding use of telework, it is considered that SSL-VPN products will become more common in the future. When using an SSL VPN product, it is necessary not only to collect vulnerability information regularly and apply a patch promptly but also to check for intrusion if a vulnerability through which authentication information might be stolen is released. You can reduce the risk of illegal access when authentication information is stolen by introducing a multi-factor authentication and enhancing authentication.

5. Malware/Ransomware

5.1. Summary of the 4th quarter of FY 2020

As in the 4th quarter of 2019, many exploitation incidents caused by ransomware including Sodinokibi, Snake and Maze have been reported.

The Quarterly Report on Global Security Trends in the 4th quarter of 2019 [42] predicted that ransomware which steals information, such as Sodinokibi and Maze, might target individuals, in particular politicians, public entertainers and celebrities. Just as predicted, celebrities were damaged by ransomware in the 4th quarter of 2020.

In May 2020, a leading law firm in the US Grubman Shire Meiselas & Sacks whose clients include many celebrities engaged in media and entertainment areas was attacked by REvil ransomware (another name of Sodinokibi), and data of their clients including singers Lady Gaga and Madonna was stolen [54]. The attacker posted 756GB of data including stolen contracts, personal information, etc. on a forum of the dark web as proof of the crime. The attacker demanded 42 million dollars as ransom money and threatened that the information will gradually be disclosed if no payment was received. Previously, attackers have simply disclosed stolen information. It is assumed that they started to threaten using information disclosure as a way to obtain money even if ransom is not paid. These are not all the methods of obtaining money for attackers. Attackers of REvil ransomware opened an auction site and sold information stolen from companies [55]. An announcement of the auction site implies that it will disclose information including that of singer Madonna stolen from the law firm. The auction of stolen confidential information is not only an alternative means of obtaining money when ransom payment is refused but also a cunning tactic which assumes that significant damage occurs when a criminal obtains personal information after the auction and demands the victim to pay ransom money. In this way, ransomware which targets personal information of celebrities with a high value of information might increase further.

Many cyberattacks which take advantage of the coronavirus pandemic have been reported in the 1st quarter of 2020. Some ransomware attackers issued a statement that they "will not attack medical institutions". However, according to the International Criminal Police Organization (INTERPOL), in reality the number of cyberattacks using ransomware rapidly increased in hospitals all over the world [56]. As the spread of the novel coronavirus has returned, cyberattacks taking advantage of the situation might expand targets from medical providers to the supply chain including research institutions, medical device manufacturers, logistics companies, etc. It is necessary to continue to take caution.

Damage from ransomware which targeted Japanese companies also occurred [57]. On June 8, automobile manufacturer Honda became a victim of a cyberattack and a world-wide system failure occurred. They were unable to use PCs in the headquarters office and it affected the company’s network system. Honda temporarily stopped the production and shipping processes in factories at home and abroad. Although details were not announced, it is assumed that Snake (EKANS) ransomware has spread over the whole company.

5.2. Example cases of attacks targeting container environments

Targets of ransomware are changing with the advancement of technology. In recent years, many organizations promote Digital Transformation (DX) and apply the use of the cloud as a means of accelerating the initiative. Above all, container technology is drawing attention, which promotes efficient development. In Docker, software which develops applications using container technology, Kinsing malware which targeted setting errors of Docker Daemon API was reported [58]. The objective of Kinsing malware was to mine (cryptomine) cryptoassets by illegally using computing resources such as CPU and memory in a container environment. Kinsing malware carries out attacks in the following procedure in Table 7.

Table 7: Attack procedure of Kinsing malware [59, 60]

#	Category	Summary
1	Intrusion	Connects to an open Docker Daemon API port.
2	Starts Container	Starts Ubuntu Container
3	Self defense	Downloads a shell script and runs the following processes. ● Configures settings so that the Container runs automatically after restarting. ● Disables security measures and clears logs. ● Stops other malware and cryptominers. Deletes files related to other malware and cryptominers. ● Force quit competitive Docker containers and deletes their images. ● Downloads Kinsing malware.
4	Runs the malware.	Runs Kinsing malware and executes the following. ● Mines (cryptomines) cryptoassets. ● Collects various information and sends it to the C&C server. ● Expands malware infection to other hosts and container environments in the same network using collected information.

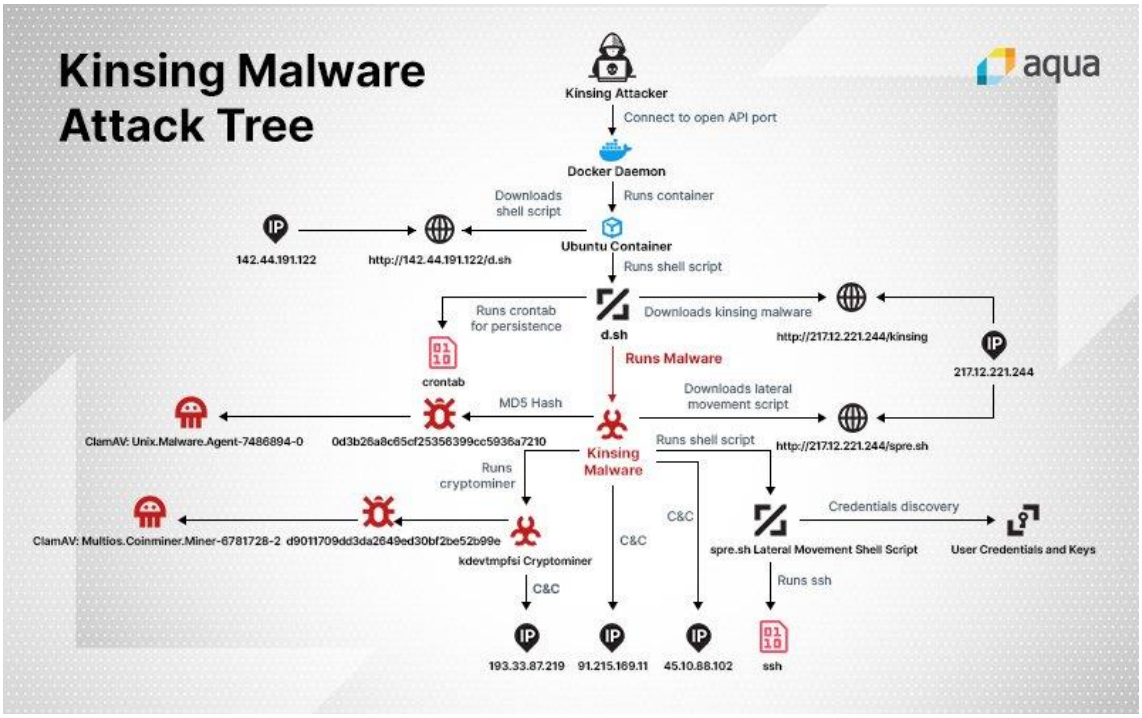


Figure 7: Attacking flow of Kinsing malware
(Source: Technical blog [58]of Aqua Security)

What makes Kinsing malware very dangerous is that it intrudes a Docker Daemon API port and takes the authority to run as root. As it uses the root authority, it can run cryptomining more effectively by changing the settings of the firewall, etc. to disable security measures, installing tools necessary for attacking and deleting competitive malware. It also runs a script to spread malware infection and expands damage to the whole container network. As Kinsing malware with the root authority is able to set up a new container, you might be charged a much higher fee if you are using a container service with a pay-as-you-go system.

Set the Docker Daemon API correctly and the container environment API to access trusted sources only as a countermeasure. The “Application Container Security Guide” (NIST SP 800-190) which is a document summarizing security risks and viewpoint of measures that are unique to containers is open to the public by the National Institute of Standards and Technology (NIST) [61]. According to this document, it is effective to configure settings of the container by limiting transmission destinations from the container and using the Center for Internet Security Docker Benchmark (CIS Benchmarks) [62] and scan the version of Kinsing malware. Scanning should be run not only when you developed a container yourself but also when you use a container which someone else has developed. We recommend running a scan continuously as the container might contain newly released vulnerabilities. For the development of applications using container technology, this document shows the standards for ensuring security. Security products for containers have been sold recently and it is useful to use such products. [63]

5.3. Other damage cases

In the 1st quarter of 2020, many organizations became a victim of malware and ransomware attacks. Many incidents caused by ransomware have been reported recently particularly from medical companies and electric power infrastructure companies. Damage cases caused by malware and ransomware which were reported in the 1st quarter of 2019 are shown in Table 8.

Table 8: Malware/ransomware damage cases * Date of announcement

Date	Target	Summary
4/6	Algeria /National oil company /Sonatrach	The whole database including confidential information leaked after being infected with ransomware. [64]
4/7 *	UK /Specialized organization of clinical trial /Hammersmith Medicines Research	Infected with Maze ransomware and the personal information of some clinical trial assistants was published between March 21-23, 2020. It has already been handled as of today. [65]
4/8 *	UK /Fintech company /Finastra	Infected with ransomware on March 20 and the customers were affected. No data breach was detected. [66]
4/9 *	UK/Foreign currency exchange agency /Travelex	Infected with Sodinobiki ransomware on December 31, 2019. The attacker demanded a ransom of 3 million dollars for encrypted files. The attacker threatened that files would be disclosed if no payment were received. Travelex announced that it paid 2.3 million dollars as ransom. [67]
4/9	USA/IT service company /Cognizant	Infected with Maze ransomware and files were stolen and encrypted. The attacker demanded ransom and threatened the company with disclosing files. [68]
4/10 *	USA/Precision part maker /Visser Precision	Infected with DoppelPaymer ransomware on March 2020. Visser Precision did not pay the ransom before the deadline at the end of March, 2020 and information was breached. The breached documents were related to Telsa, Lockheed Martin, Boeing and SpaceX. [69]
4/14 *	Portugal/Energy company /EDP	Infected with Ragnar Locker ransomware. The attacker claimed that he stole confidential information exceeding 10TB and threatened that all the stolen data would be disclosed if a 1,580BTC ransom were not paid. [70]

4/18	USA/IT service company /Cognizant	The internal system was infected with Maze ransomware and some services for customers stopped. [71]
4/21 *	USA/Torrance City	Infected with DoppelPaymer ransomware. The attacker claimed that he stole more than 200GB of confidential information including the city's budget information and demanded a 100BTC ransom. [72]
4/22	Kanagawa Prefecture/Kawasaki Municipal High School	The school network server was infected with ransomware and files in the server were encrypted. The school had been infected with another ransomware on October 2019. Security measures had been strengthened. The ransomware which the school was infected with this time was different from the previous case. [73]
4/24 *	USA/Video distribution software company/SeaChange International	Infected with Sodinobiki ransomware. The attacker claimed that he stole confidential information before encrypting the system. [74]
4/26 *	USA/Pharmaceutical company /ExecuPharm	Infected with CLOP ransomware on March 13. The attacker disclosed the stolen information on a dark web site. [75]
4/28 *	UK/Construction design company/Zaha Hadid Architects	Infected with ransomware. The attacker stole files and encrypted them. The attacker demanded a ransom and threatened that files would be disclosed if no payment were received. [76]
4/28 *	USA/Biopharmaceutical company /ExecuPharm	Infected with CLOP ransomware on March 13. Demanded a ransom and some stolen corporate and personal information was disclosed. [77]
5/5	Australia/Logistics company /Toll Group	Infected with Nefilim ransomware subvariety. Part of the system stopped but files were recovered using backups. The company was infected with MailTo ransomware on February 3. [78]
5/6	Germany/Hospital operating company/Fresenius Group	Infected with Snake ransomware. The following day of infection, a threatening letter arrived which said that the stolen database and documents would be disclosed if no payment or contact were received within 48 hours. [79]
5/7	USA/Texas /Office of Court Administration	Infected with ransomware. The Courts showed their intention to refuse to pay the ransom. [80]
5/11	USA/ATM maker /Diebold Nixdorf	Infected with ProLock ransomware. The Courts showed their intention to refuse to pay the ransom. [81]

5/13 *	USA/Healthcare management company /Magellan Health	Infected with ransomware. Information was stolen but there was no trace of exploitation. [82]
5/19	Australia /Steel manufacturer /BlueScope Steel	Infected with ransomware and some production and sales operations were affected. [83]
5/24	USA/Semiconductor manufacturer /MaxLinear	Infected with Maze ransomware. There was no large influence on the company's operation. Some confidential information was disclosed online. [84]
5/26	USA/Alabama /Florence City	Infected with ransomware and the internal IT network stopped. The city decided to pay 300,000 bitcoins to the attacker in the Diet. [85]
5/28	USA/University of Michigan	Infected with Netwalker ransomware. The attacker disclosed the stolen files on a leak site because the university refused to pay a ransom. [86]
6/2 *	UK /Electric power company/Elexon	Infected with Sodinokibi ransomware and the internal IT network was affected. The attacker disclosed the stolen files on a leak site. [87]
6/3	USA/University of California, San Francisco	Infected with Netwalker ransomware. The university paid bitcoin equivalent to 1.14 million dollars to the attacker. [88]
6/3	USA/Intercontinental ballistic missile maintenance agency /Westech International	Infected with Maze ransomware and some files were encrypted. It is unclear whether confidential information of the army was stolen. [89]
6/9	Australia /Beverage maker /Lion	Infected with ransomware. The company stopped the IT system to prevent the spread of infection, which affected product shipping and caused delays. Document lists of the company and some confidential information were disclosed. [90]
6/11	Italy /Electric power company/Enel Group	Infected with Snake ransomware and the internal IT network was affected. [91]
6/11	USA/Consulting company /Threadstone Advisors	Infected with Maze ransomware. The attacker stole files and then encrypted them. The company is an American consulting company with clients including Victoria Beckham, a former member of the Spice Girls. [92]
6/25 *	South Korea /General home electric appliance manufacturer /LG Electronics	Infected with Maze ransomware. The attacker stole 40GB of source code. [93]

6. Outlook

New risk of communications from using online meeting tools

This document has introduced points which users should be aware of when using Zoom. Business communications which have previously been performed in person by gathering in the same place will be increasingly replaced by methods using online tools including Zoom. However, we should not forget that the spread of online communications which allows anyone to connect anywhere can generate new risks we were not conscious of before. For example, sales people of the existing companies exchanged business cards and gain trust in person to sell commercial materials and services. When this activity is performed online, it is easy to carry out fraud and swindles. It is considered that, as online activities become more and more common, people will become less cautious about being approached by strangers, which will make it easier for attackers to launch attacks. When promoting online communications, one needs to understand the risk of fraud and swindles and prepare a way of authenticating identity and information reliability.

Increasing number of attacks targeting a vulnerability of VPN products

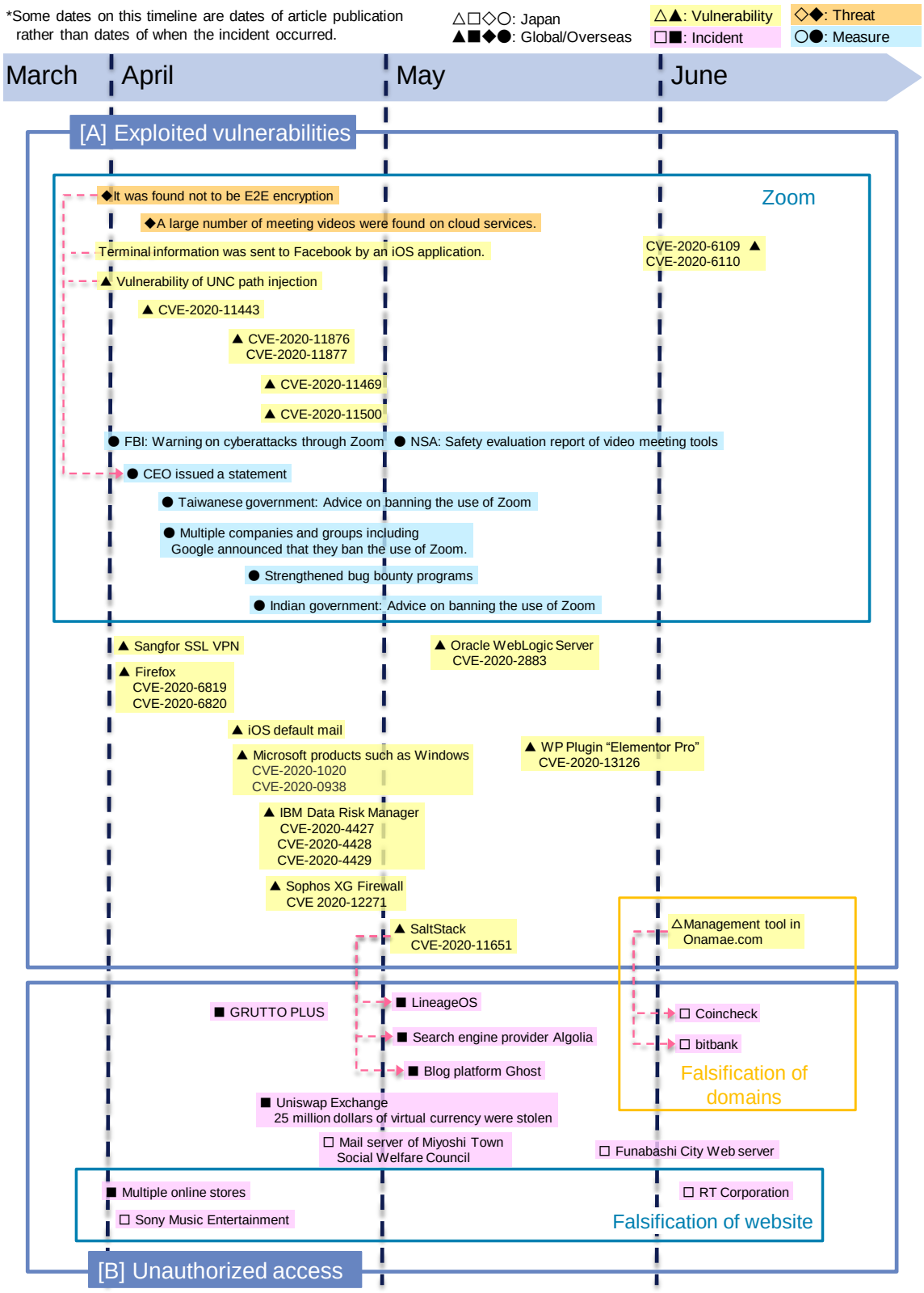
According to an investigation by Skybox Security [94], about 9000 vulnerabilities were reported in the first half of 2020. The number is likely to reach a record high of 20,000 in 2020. Following the impact of the novel coronavirus spread, the use of telework will expand and VPN products will spread rapidly. Taking this into account, it is considered that the number of attacks targeting a vulnerability of VPN products will increase. Vulnerabilities of VPN products allow code running and authentication information stealing remotely. Therefore, the time between the publishing of a vulnerability and the occurrence of intrusion after a cyberattack tends to be shorter. If you are using a VPN product, collect information on the product's vulnerabilities and check details. If the vulnerability can be accessible from a third party on the Internet, apply the patch within a few days or temporarily stop the use of the VPN product.

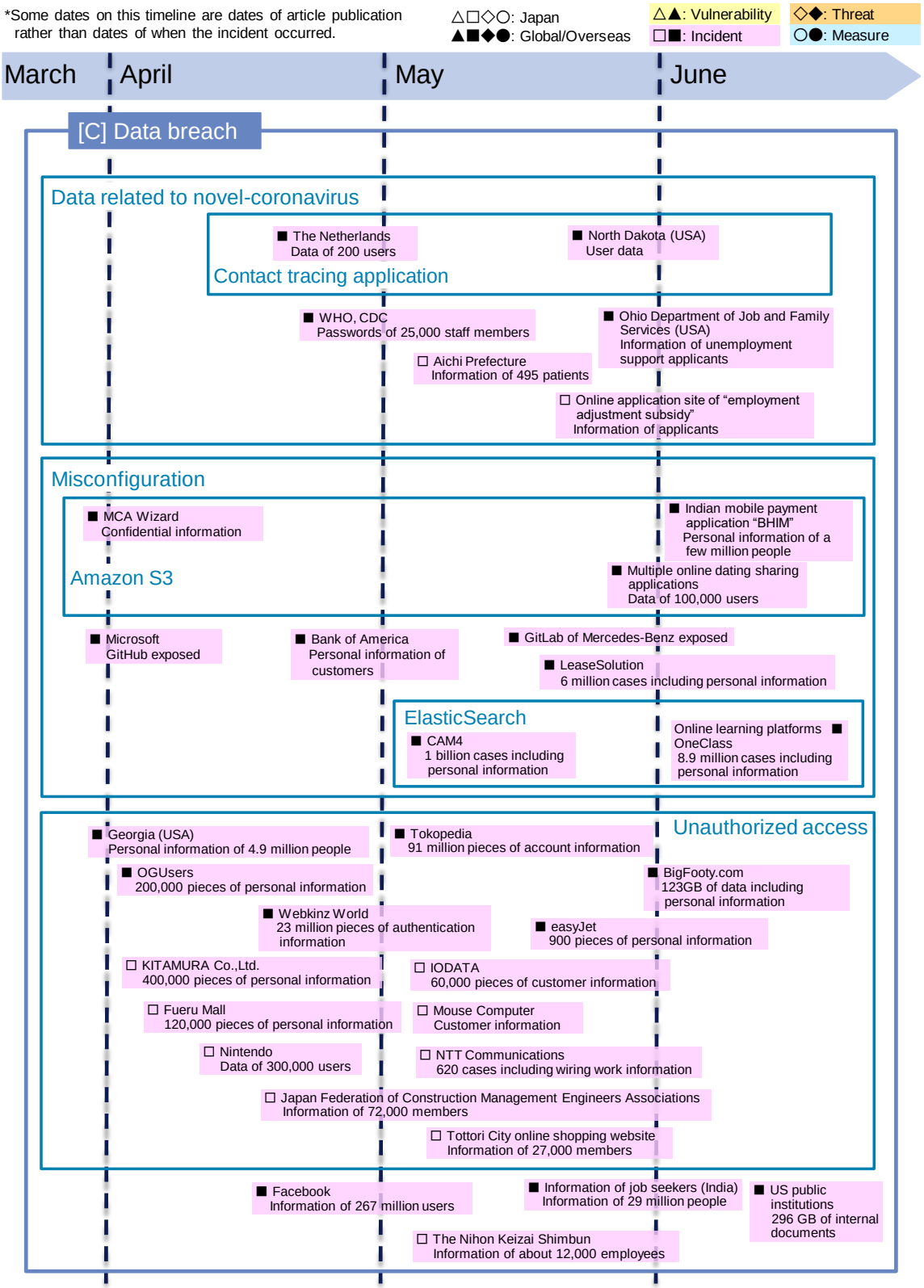
Increase in the number of attack cases targeting Docker

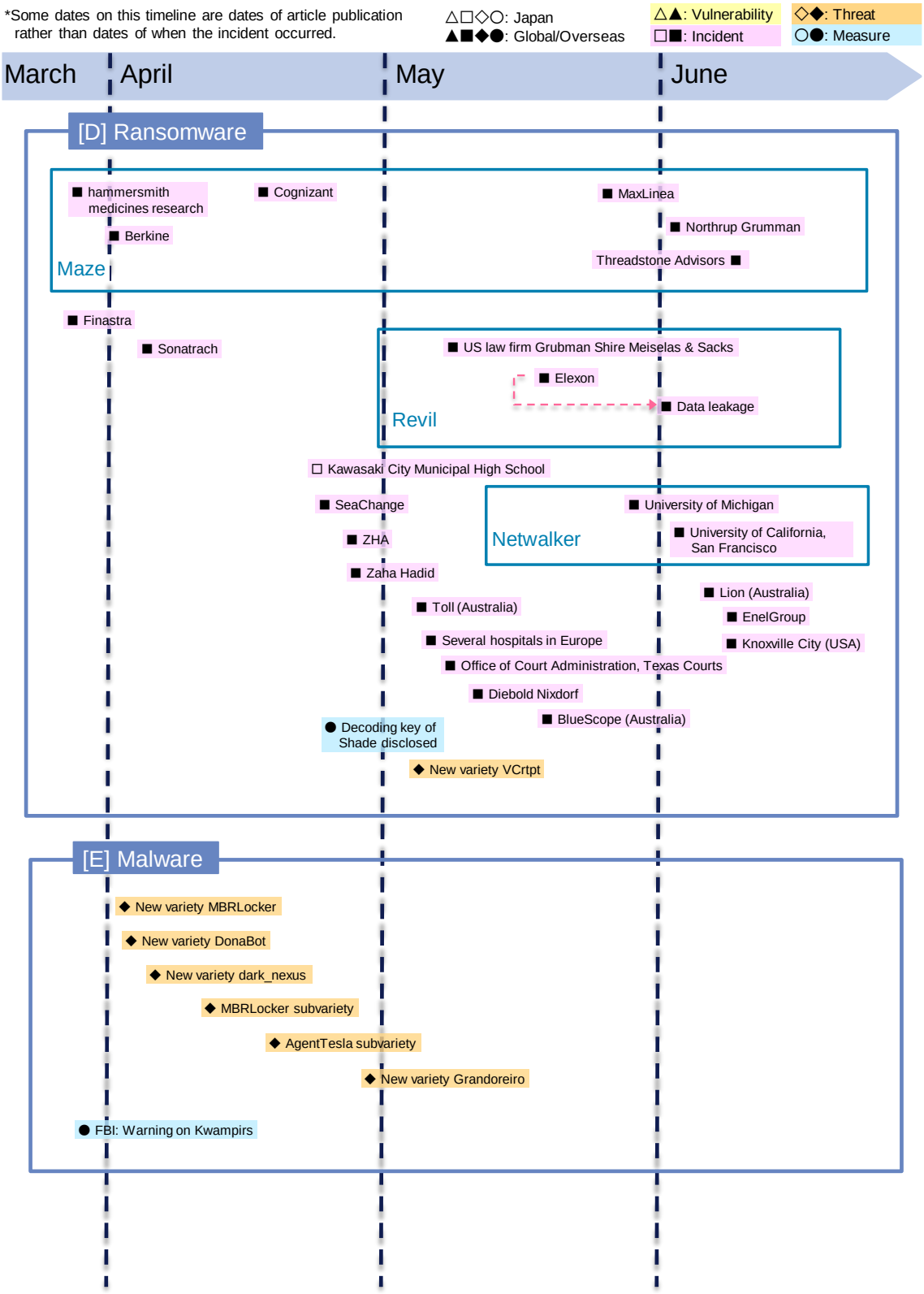
It is assumed that, if demands of cloud services increase due to the expanding digital transformation and telework, the use of Docker will increase subsequently [95]. As the use of Docker increases, the number of Dockers with insufficient security measures is likely to increase, and so are attacks targeting at such Dockers.

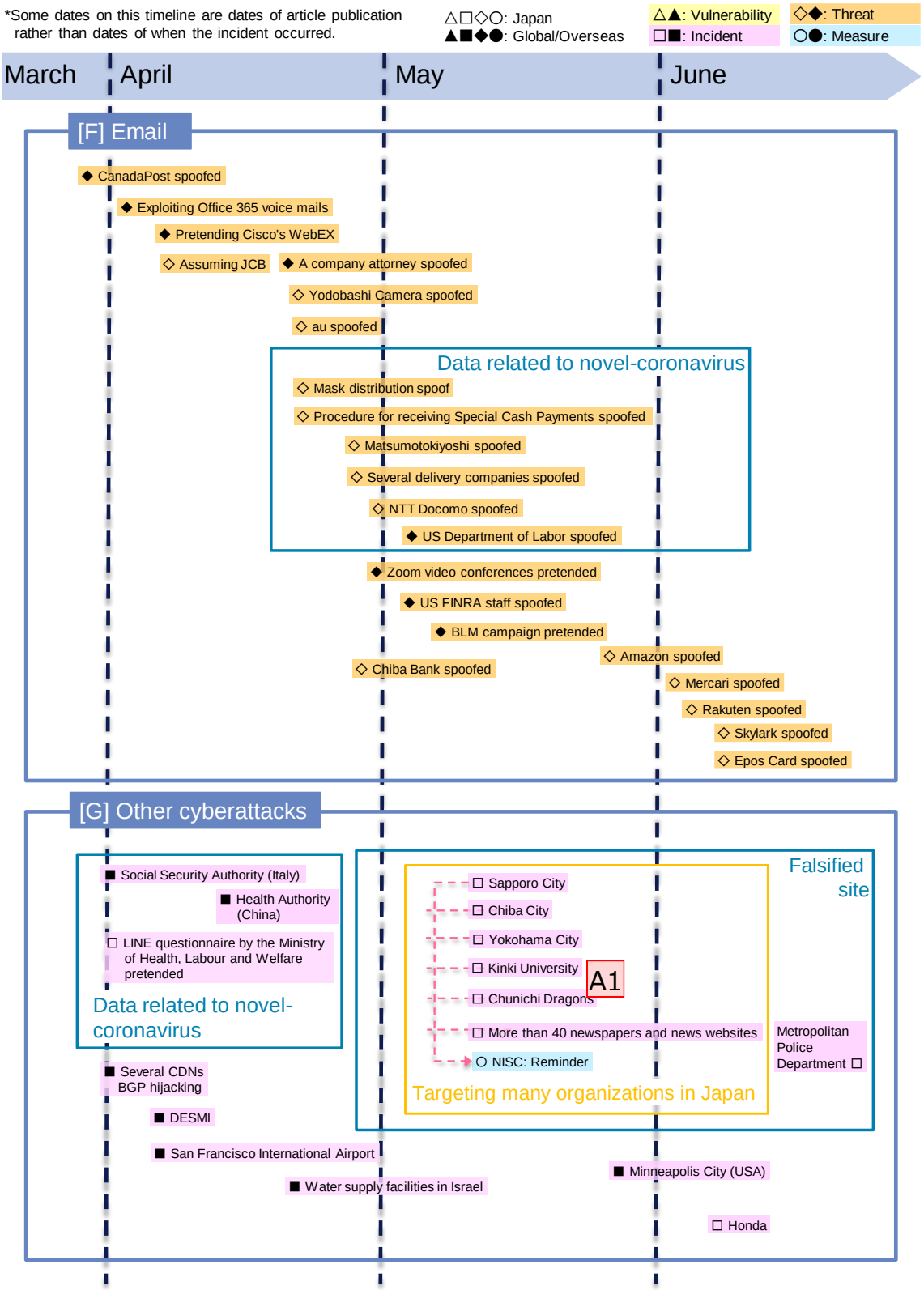
Attacks intruding into Docker include not only those introduced in “5. Malware/Ransomware” but also those targeting the setting errors and vulnerabilities of container orchestra tools such as Kubernetes, etc., those distributing a Docker image which contains malware and those placing malware inside containers by exploiting the vulnerabilities and setting errors of the tool used when Docker is developed using containers [96] [97]. To respond to these various attacks, it is recommended to scan the settings of the Docker you are currently using or will use by using the “Application Container Security Guide” (NIST SP 800-190) [61] or Center for Internet Security Docker Benchmark (CIS Benchmarks) [62] and take measures after clarifying setting rule violations and setting errors.

7. Timeline









References

[1] “Businesses @ Work (From Home) 2020,” Okta, 29 5 2020. [オンライン]. Available: https://www.okta.com/businesses-at-work/2020/work-from-home/.

[2] “Zoom is Now Worth More Than the World’s 7 Biggest Airlines,” Visual Capitalist, 15 5 2020. [オンライン]. Available: https://www.visualcapitalist.com/zoom-boom-biggest-airlines/.

[3] “Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account,” Motherboard, 26 3 2020. [オンライン]. Available: https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

[4] “Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing.,” The Intercept, 31 3 2020. [オンライン]. Available: https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

[5] “ JVN iPedia 脆弱性対策情報対策データベース,” IPA, [オンライン]. Available: https://jvndb.jvn.jp/.

[6] “Talos Vulnerability Report,” Cisco, 3 6 2020. [オンライン]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055.

[7] “Attackers can use Zoom to steal users’ Windows credentials with no warning,” WIRED Media Group, 2 4 2020. [オンライン]. Available: https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentials-with-no-warning/.

[8] “Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links,” Bleeping Computer, 31 3 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/.

[9] “Zoom利用者へのメッセージ,” Zoom, 1 4 2020. [オンライン]. Available: https://blog.zoom.us/ja/a-message-to-our-users/.

[10] “Zoom sued by shareholder for ‘overstating’ security claims,” Techcrunch, 9 4 2020. [オンライン]. Available: https://techcrunch.com/2020/04/08/zoom-sued-shareholder-security/.

[11] “Move Fast and Roll Your Own Crypto,” Citizen Lab, 3 4 2020. [オンライン]. Available: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

[12] “トロント大学 Citizen Lab研究へのレスポンス,” Zoom, 3 4 2020. [オンライン]. Available: https://blog.zoom.us/ja/response-to-research-from-university-of-torontos-citizen-lab/.

[13] “Zoomの iOS クライアントでのFacebook SDK 利用について (翻訳版),” Zoom, 27 3 2020. [オンライン]. Available: https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/zoom-use-of-facebook-sdk-in-ios-client.

[14] “Zoom’s Privacy Policy,” Zoom, 29 3 2020. [オンライン]. Available: https://blog.zoom.us/zoom-privacy-policy/.

[15] “Zoom Privacy Lawsuit,” Wexler Wallace, [オンライン]. Available: https://www.wexlerwallace.com/zoom-privacy-lawsuit/.

[16] “Zoom’s Waiting Room Vulnerability,” Citizen Lab, 8 4 2020. [オンライン]. Available: https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/.

[17] “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic,” FBI, 30 3 2020. [オンライン]. Available: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[18] “Executive Yuan orders agencies to step up video conferencing security,” Executive Yuan, 7 4 2020. [オンライン]. Available: https://english.ey.gov.tw/Page/61BF20C3E89B856/849887da-0aa7-4b84-8fba-1b6b1183843f.

[19] “MHA issues Advisory on Secure use of ZOOM Meeting Platform,” Ministry of Home Affairs, 16 4 2020. [オンライン]. Available: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1615008.

[20] “India records highest Zoom installs in Q1 2020: Sensor Tower,” TechCircle, 17 4 2020. [オンライン]. Available: https://www.techcircle.in/2020/04/17/india-records-highest-zoom-installs-in-q1-2020-sensor-tower.

[21] “Government selects 10 Indian companies to develop Desi Zoom rival,” GADGETS NOW, 25 5 2020. [オンライン]. Available: https://www.gadgetsnow.com/tech-news/government-selects-10-indian-companies-to-develop-desi-zoom-rival/articleshow/75965854.cms.

[22] “Google Told Its Workers That They Can’t Use Zoom On Their Laptops Anymore,” BuzzFeed, 8 4 2020. [オンライン]. Available: https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom.

[23] “Web会議サービスを使用する際のセキュリティ上の注意事項,” IPA, 14 7 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/webmeeting.html.

[24] C. Point, “As organizations get back to business, cyber criminals look for new angles to exploit,” Check Point, 6 2020. [オンライン]. Available: https://blog.checkpoint.com/2020/06/25/as-organizations-get-back-to-business-cyber-criminals-look-for-new-angles-to-exploit/.

[25] M. BRENAN, “U.S. Workers Discovering Affinity for Remote Work,” Gallup, 3 4 2020. [オンライン]. Available: https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx.

[26] Shodan, “Trends in Internet Exposure,” Shodan, 29 3 2020. [オンライン]. Available: https://blog.shodan.io/trends-in-internet-exposure/.

[27] T. Roccia, “Cybercriminals Actively Exploiting RDP to Target Remote Organizations,” McAfee, 6 5 2020. [オンライン]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cybercriminals-actively-exploiting-rdp-to-target-remote-organizations/.

[28] S. Gatlan, “RDP brute-force attacks are skyrocketing due to remote working,” BleepingComputer, 29 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/rdp-brute-force-attacks-are-skyrocketing-due-to-remote-working/.

[29] D. Galov, “Remote spring: the rise of RDP bruteforce attacks,” Kaspersky, 29 4 2020. [オンライン]. Available: https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/.

[30] O. Kubovič, “Remote access at risk: Pandemic pulls more cyber-crooks into the brute-forcing game,” ESET, 29 6 2020. [オンライン]. Available: https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/.

[31] Abnormal Security, “Abnormal Attack Stories: VPN Impersonation Phishing,” Abnormal Security, 3 6 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-vpn-impersonation-phishing/.

[32] Abnormal Security, “Abnormal Attack Stories: Zoom Phishing,” Abnormal Security, 21 4 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-zoom-phishing/.

[33] Abnormal Security, “Abnormal Attack Stories: Microsoft Teams Impersonation,” Abnormal Security, 1 5 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/.

[34] Abnormal Security, “Abnormal Attack Stories: Cisco Webex Phishing,” Abnormal Security, 5 5 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-cisco-webex-phishing/.

[35] Trend Micro, “Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers,” Trend Micro, 21 5 2020. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers/.

[36] avast, “アバスト、「フリースウェア」と見られるiOS VPNアプリをApp Storeで発見,” avast, 17 6 2020. [オンライン]. Available: https://press.avast.com/ja-jp/avast-warns-of-fleeceware-apps.

[37] B. BARRETT, “Hack Brief: An Adult Cam Site Exposed 10.88 Billion Records,” WIRED, 5 5 2020. [オンライン]. Available: https://www.wired.com/story/cam4-adult-cam-data-leak-7tb/.

[38] J. Yeung, “Almost entire population of Ecuador has data leaked,” CNN, 17 9 2019. [オンライン]. Available: https://edition.cnn.com/2019/09/17/americas/ecuador-data-leak-intl-hnk-scli/index.html#:~:text=More%20than%2020%20million%20people,population%20could%20have%A20been%20affected..

[39] S. WHITE, “Honda struck by 40GB data breach,” PrivSec, 1 8 2019. [オンライン]. Available: https://gdpr.report/news/2019/08/01/honda-struck-by-40gb-data-breach/.

[40] ナカバヤシ株式会社, “弊社が運営する「フエルモール」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ【続報】,” ナカバヤシ株式会社, 3 6 2020. [オンライン]. Available: https://www.nakabayashi.co.jp/news/2020/info/715.

[41] NTTコミュニケーションズ, “当社への不正アクセスによる情報流出の可能性について,” NTTコミュニケーションズ, 28 5 2020. [オンライン]. Available: https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html.

[42] 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4四半期,” 26 06 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_4q_securityreport.pdf.

[43] C. Cimpanu, “Mercedes-Benz onboard logic unit (OLU) source code leaks online,” ZDNet, 18 5 2020. [オンライン]. Available: https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/.

[44] T. Brewster, “EasyJet Hacked For Four Months, Data On 9 Million Customers And 2,000 Credit Cards Stolen,” Forbs, 19 5 2020. [オンライン]. Available: https://www.forbes.com/sites/thomasbrewster/2020/05/19/easyjet-hacked-9-million-customers-and-2000-credit-cards-hit/#77d7441f1ae1.

[45] 任天堂株式会社, “「ニンテンドーネットワークID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い,” 任天堂株式会社, 9 6 2020. [オンライン]. Available: https://www.nintendo.co.jp/support/information/2020/0424.html.

[46] 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年度版 第2四半期）,” 29 8 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[47] U. S. C. E. R. Team, “Alert (AA20-107A),” 22 4 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-107a.

[48] P. Secure, “SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX,” 24 4 2019. [オンライン]. Available: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101.

[49] B. Packets, “Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510,” 24 8 2019. [オンライン]. Available: https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/.

[50] 一. J. コーディネーションセンター, “複数の SSL VPN 製品の脆弱性に関する注意喚起,” 6 9 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[51] U. S. C. E. R. Team, “Alert (AA20-010A),” 10 1 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-010a.

[52] tenable, “CVE-2019-11510: 「緊急」の Pulse Connect Secure の脆弱性、ランサムウェア「Sodinokibi 」の攻撃に悪用される,” 7 1 2020. [オンライン]. Available: https://jp.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware.

[53] 衛. 亮介, “Pulse Connect Secure の脆弱性を狙った攻撃事案,” 26 3 2020. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html.

[54] CBS Interactive, “REvil ransomware gang launches auction site to sell stolen data,” 2 6 2020. [オンライン]. Available: https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/.

[55] Graham Cluley, “Malicious Coronavirus victim tracking app demands ransom payment from Android users,” 16 3 2020. [オンライン]. Available: https://www.grahamcluley.com/coronavirus-android-ransomware/.

[56] Data Breach TODAY, “No COVID-19 Respite: Ransomware Keeps Pummeling Healthcare,” 7 4 2020. [オンライン]. Available: https://www.databreachtoday.com/no-covid-19-respite-ransomware-keeps-pummeling-healthcare-a-14072.

[57] 朝日新聞, “ホンダ、サイバー攻撃被害認める　身代金ウイルス拡大か,” 9 6 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN6966YFN69ULFA03G.html.

[58] Aqua Security, “Threat Alert: Kinsing Malware Attacks Targeting Container Environments,” 3 4 2020. [オンライン]. Available: https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability.

[59] CREATIONLINE, INC, “脅威：コンテナ環境を対象としたマルウェア「Kinsing」が増加中 #AquaSecurity #セキュリティ #コンテナ #マルウェア,” 8 4 2020. [オンライン]. Available: https://www.creationline.com/lab/34036.

[60] Trend Micro Incorporated, “Docker デーモンのオープンポートを狙うマルウェア、目的はボット感染とマイニング,” 16 7 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/25580.

[61] National Institute of Standards and Technology, “Application Container Security Guide,” 9 2017. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf.

[62] Center for Internet Security, [オンライン]. Available: https://www.cisecurity.org/cis-benchmarks/.

[63] NTT DATA Corporation, “注目を集める仮想化技術「コンテナ」、そのセキュリティ対策とは？,” 31 1 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/data-insight/2019/0131/.

[64] HACKREAD, “Maze ransomware group hacks oil giant; leaks data online,” 6 4 2020. [オンライン]. Available: https://www.hackread.com/maze-ransomware-group-hacks-oil-giant-leaks-data/.

[65] Bleeping Computer LLC, “Drug testing firm sends data breach alerts after ransomware attack,” 7 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/drug-testing-firm-sends-data-breach-alerts-after-ransomware-attack/.

[66] Krebs on Security, “Security Breach Disrupts Fintech Firm Finastra,” 8 4 2020. [オンライン]. Available: https://krebsonsecurity.com/2020/03/security-breach-disrupts-fintech-firm-finastra/.

[67] Security Affairs by Pierluigi Paganini, “Travelex paid $2.3 Million ransom to restore after a ransomware attack,” 9 4 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/101339/cyber-crime/travelex-paid-ransomware.html.

[68] Bleeping Computer LLC, “IT giant Cognizant confirms data breach after ransomware attack,” 17 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/.

[69] Biting the hand that feeds IT, “Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay,” 10 4 2020. [オンライン]. Available: https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/.

[70] Bleeping Computer LLC, “RagnarLocker ransomware hits EDP energy giant, asks for €10M,” 14 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/.

[71] Sophos Ltd, “Maze ransomware hits US giant Cognizant,” 20 4 2020. [オンライン]. Available: https://nakedsecurity.sophos.com/2020/04/20/maze-ransomware-hits-us-giant-cognizant/.

[72] Bleeping Computer LLC, “DoppelPaymer Ransomware hits Los Angeles County city, leaks files,” 21 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-los-angeles-county-city-leaks-files/.

[73] NEWSGAIA, “高校でランサム被害、セキュリティ強化するも再発 - 川崎市,” 8 5 2020. [オンライン]. Available: http://www.security-next.com/114691.

[74] Security Affairs by Pierluigi Paganini, “SeaChange video delivery software solutions provider hit by Sodinokibi ransomware,” 24 4 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/102177/cyber-crime/seachange-sodinokibi-ransomware.html.

[75] Verizon Media, “Hackers publish ExecuPharm internal data after ransomware attack,” 28 4 2020. [オンライン]. Available: https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/.

[76] CBS Interactive, “Hackers threaten to leak data from high-end architecture firm Zaha Hadid,” 28 4 2020. [オンライン]. Available: https://www.zdnet.com/article/hackers-threaten-to-leak-data-from-high-end-architecture-firm-zaha-hadid/?mid=1#cid=734236.

[77] MediaOps Inc, “Cybercriminals Leak ExecuPharm Internal Documents After Ransomware Attack,” 28 4 2020. [オンライン]. Available: https://securityboulevard.com/2020/04/cybercriminals-leak-execupharm-internal-documents-after-ransomware-attack/.

[78] rootdaemon, “Logistics giant Toll Group hit by ransomware for the second time in three months,” 6 5 2020. [オンライン]. Available: https://rootdaemon.com/2020/05/06/logistics-giant-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/.

[79] Bleeping Computer LLC, “Large scale Snake Ransomware campaign targets healthcare, more,” 6 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/large-scale-snake-ransomware-campaign-targets-healthcare-more/.

[80] CBS Interactive, “Texas courts slammed by ransomware attack,” 12 5 2020. [オンライン]. Available: https://www.zdnet.com/article/texas-courts-slammed-by-ransomware-attack/.

[81] Krebs on Security, “Ransomware Hit ATM Giant Diebold Nixdorf,” 20 5 2020. [オンライン]. Available: https://krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/.

[82] CyberRisk Alliance, LLC, “Magellan Health warns ransomware attack exposed PII,” 13 5 2020. [オンライン]. Available: https://www.scmagazine.com/home/security-news/magellan-health-warns-ransomware-attack-exposed-pii/.

[83] Security Affairs by Pierluigi Paganini, “Australian product steel producer BlueScope hit by cyberattack,” 19 5 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/103453/cyber-crime/bluescope-cyber-attack.html/.

[84] Reuters, “Chipmaker MaxLinear hit by 'Maze' ransomware attack,” 16 6 2020. [オンライン]. Available: https://www.reuters.com/article/us-maxlinear-cyber/chipmaker-maxlinear-hit-by-maze-ransomware-attack-idUSKBN23N243.

[85] Wells Media Group, Inc, “Alabama City to Pay $300K in Bitcoin Ransom in Computer System Hack,” 12 6 2020. [オンライン]. Available: https://www.insurancejournal.com/news/southeast/2020/06/12/572046.htm.

[86] Bleeping Computer LLC, “Netwalker ransomware continues assault on US colleges, hits UCSF,” 3 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/.

[87] Security Affairs by Pierluigi Paganini, “Sodinokibi ransomware operators leak files stolen from Elexon electrical middleman,” 2 6 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/104149/cyber-crime/sodinokibi-published-elexon-files.html.

[88] CyberRisk Alliance, “UCSF paid $1.4 million ransom in NetWalker attack,” 29 6 2020. [オンライン]. Available: https://www.scmagazine.com/home/security-news/ucsf-paid-1-4-million-ransom-in-netwalker-attack/.

[89] Sophos Ltd., “Nuclear missile contractor hacked in Maze ransomware attack,” 4 6 2020. [オンライン]. Available: https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack.

[90] CBS Interactive, “Lion warns of beer shortages following ransomware attack,” 12 6 2020. [オンライン]. Available: https://www.zdnet.com/article/lion-warns-of-beer-shortages-following-ransomware-attack/.

[91] Bleeping Computer LLC, “Power company Enel Group suffers Snake Ransomware attack,” 11 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/.

[92] Reed Exhibitions Ltd, “MAZE Attacks Victoria Beckham's Advisory Firm,” 11 6 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/news/maze-attacks-victoria-beckhams/?&web_view=true.

[93] Bleeping Computer LLC, “LG Electronics allegedly hit by Maze ransomware attack,” 25 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/lg-electronics-allegedly-hit-by-maze-ransomware-attack/.

[94] P. Muncaster, “Experts Predict Record 20,000 CVEs for 2020,” 21 7 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/profile/phil-muncaster/.

[95] Grand View Research, “アプリケーションコンテナーの市場規模| グローバル産業レポート、2019-2025,” Grand View Research, [オンライン]. Available: https://www.grandviewresearch.com/industry-analysis/application-container-market.

[96] 宮田健, “「コンテナセキュリティ」とは――コンテナを活用する人が知っておくべき6つのポイント,” @IT, 16 10 2019. [オンライン]. Available: https://www.atmarkit.co.jp/ait/articles/1910/16/news015_2.html.

[97] J. Chen, “セキュアでないDockerデーモンへの攻撃者の戦術とテクニックが明らかに 地理的分布で日本は全体の3.7%,” パロアルトネットワークス株式会社, 30 1 2020. [オンライン]. Available: https://unit42.paloaltonetworks.jp/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/.

NTT DATA
Trusted Global Innovator

Published on Friday, September 11, 2020

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Ryo Hoshino / Takayuki Aoki / Tomohiro Ito / Daisuke Miyazaki / Jun Kinoshita / Risa Shishido / Kazuki Shimizu
nttdata-cert@kits.nttdata.co.jp