NTT DATA
Trusted Global Innovator

# Quarterly Report on Global Security Trends

## 2nd Quarter of 2019

# Table of Contents

1. Executive Summary.......1
2. Featured Topics.......2
2.1. Supply Chain Attack.......2
3. Data Breach.......7
4. Vulnerability.......10
4.1. Vulnerabilities of Some SSL/VPN Products.......10
4.2. Other Exploited Vulnerabilities.......11
5. Malware/Ransomware.......13
6. Outlook.......17
7. Timeline.......19
References.......25

# 1. Executive Summary

In this report, NTTDATA-CERT surveys and analyzes quarterly global trends from its own perspective based on cybersecurity-related information collected in the survey/analysis period.

## Supply Chain Attack

During 2nd Quarter of FY2019, a supply chain attack came to an issue once again. The case where Sprint was especially characteristic, attackers marked the case in which boundary of responsibility for security between each organization was unspecific, exploited intersystem coordination on website, and used measures to abstract customer information through "samsung.com". Therefore, it is common challenge for the people engaged in security to explore the best practice against those attacks.

## Automation of Web Skimming

Such as database system, multiple data breach related to misconfiguration have been occurring. Moreover, the method of web skimming confirmed for some time has changed. Attackers automatically have searched and efficiently have attacked an EC site on a cloud service that has misconfiguration, then have stolen information of a credit card by injecting web skimming scripts on EC site.

## Ransomware Incidents in the USA

Since April 2019, Ransomware incidents have continued to occur. A number of Ransomware incidents have been reported in 2nd Quarter of FY2019. In addition to local governments, some schools and hospitals have also attacked by Ransomware, thus the said incidents have occurred at public institutions on a wide scale. As an example of Ransomware infection, the method of attack called, "Triple Threat" combined three types of malware, "Emotet", "Trickbot", and "Ryuk" have been found.

## Outlook

Such as misconfiguration, attacks marked vulnerability, email attacks for malware distributions, and Ransomware attacks, etc., attacks confirmed for some time will get more sophisticated methods and continue. Attackers will try to make cyberattacks succeed by misconfiguration on cloud service, automatic searching for vulnerability, sending attack mails that cannot be identified whether official ones. Therefore, the same measures as before is likely to increase the incidents.

# 2. Featured Topics

## 2.1. Supply Chain Attack

Supply chain attack is the word that indicates two types of attack methods nowadays. [1]
First method, organizations whose security measures are optimistic act as stepping stone to attack on supply chain such as clients, etc. in order to attack the target organizations such as big companies and government organizations, etc.
Second method, the distributions of software injecting malwares and attacking codes act as stepping stone to attacks through software supply chains such as software developers and distributors, etc. This method is covered as Featured Topics on "Quarterly Report on Global Security Trends 1st Quarter of 2019". [2]
In 2nd Quarter of FY2019, the supply chain attack above described as First method came to an issue once again.

Table 1：Supply chain attacks occurred and reported in 2nd Quarter of FY2019

| No. | Date | Via | Summary |
|---|---|---|---|
| 1 | 7/13 | Contractor : SyTech | News media ZDNet reported that information of Federal Security Service of the Russian Federation as intelligence agency in Russia was stolen from SyTech Corp. entrusted its business by an attacker. [3] The identity of the attacker was the hacking group "0v1ru$", who stole classified information of 7.5GB by access to the project management tool JIRA and Active Directory server. The stolen classified information was then shared with another hacking group "Digital Revolution". |
| 2 | 7/22 | Samsung.com | News media ZDNet reported that personal data breach occurred on Sprint Corp., the communications company in the USA, due to unauthorized access to Sprint via the official site of Samsung group "samsung.com". [4]<br>With regard to sending emails from Sprint to users impacted by this incident, an attacker has illegally accessed to users' Sprint accounts via the web page for new line contract "add a line". [5] |

| No. | Date | Via | Summary |
|---|---|---|---|
| 3 | 9/18 | IT service company | Symantec Corp. disclosed that the attack group “Tortoiseshell” has been attacking the IT service company of Saudi Arabia since July 2018 to act as a stepping stone to supply chain attack on its official blog. [6]<br>11 organizations using the said IT service company were attacked by Tortoiseshell, at least domain controller servers for two of those organizations were injected information collecting tools on. |

The notable example in incidents of Table 1 is the one of “Sprint”, which is the second biggest communications company in the USA. In this case, attackers did not directly attack on Sprint’s web site, invade into inside, and steal its customer information, but once they invaded into the group company’s web site of Samsung group, took a detour, and stole Sprint’s customer information.

According to the article reported by news media ZDNet and the contents that Sprint reported to customers impacted by its incident, an attacker has illegally accessed via “add a line” that is the web page for new line contract in samsung.com.

In common usage, it seems that the cooperation like Figure 1 executed between the site of samsung.com and Sprint.

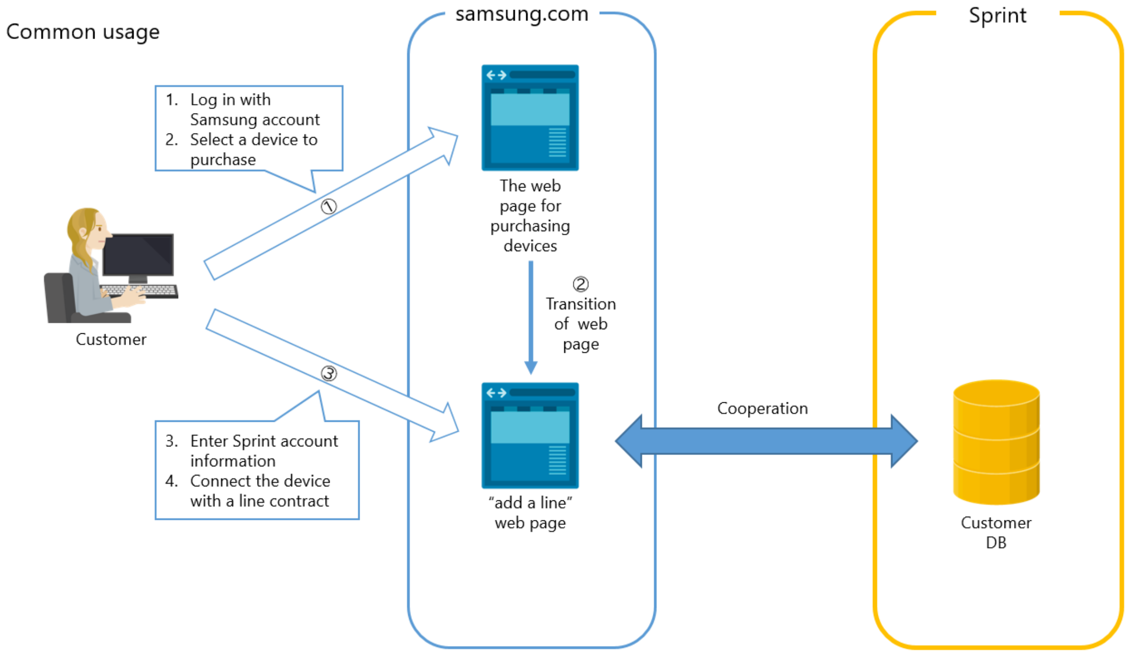

Common usage
samsung.com
Sprint
1. Log in with Samsung account
2. Select a device to purchase
①
The web page for purchasing devices
② Transition of web page
Customer
③
3. Enter Sprint account information
4. Connect the device with a line contract
“add a line” web page
Cooperation
Customer DB

Figure 1： Flow diagram of access in common usage

## Flow of Access in Common Usage

① Access to the web page for purchasing devices

1. A customer logs in “samsung.com” with their own Samsung account
2. Select a device on the web page of samsung.com for purchasing devices

② Make a transition from the web page for purchasing devices to “add a line” web page

③ Access to add a line web page after taking over the state of login samsung.com

3. Enter the Sprint account information of a customer (ID and password)

④ After the user authentication is successful, the user information is shared between samsung.com and Sprint. Linked the purchased device and the line contract

4. The Customer can see the information of their line contract

Meanwhile, it seems that the incident in this time was performed with the flow of Figure 2 as below.

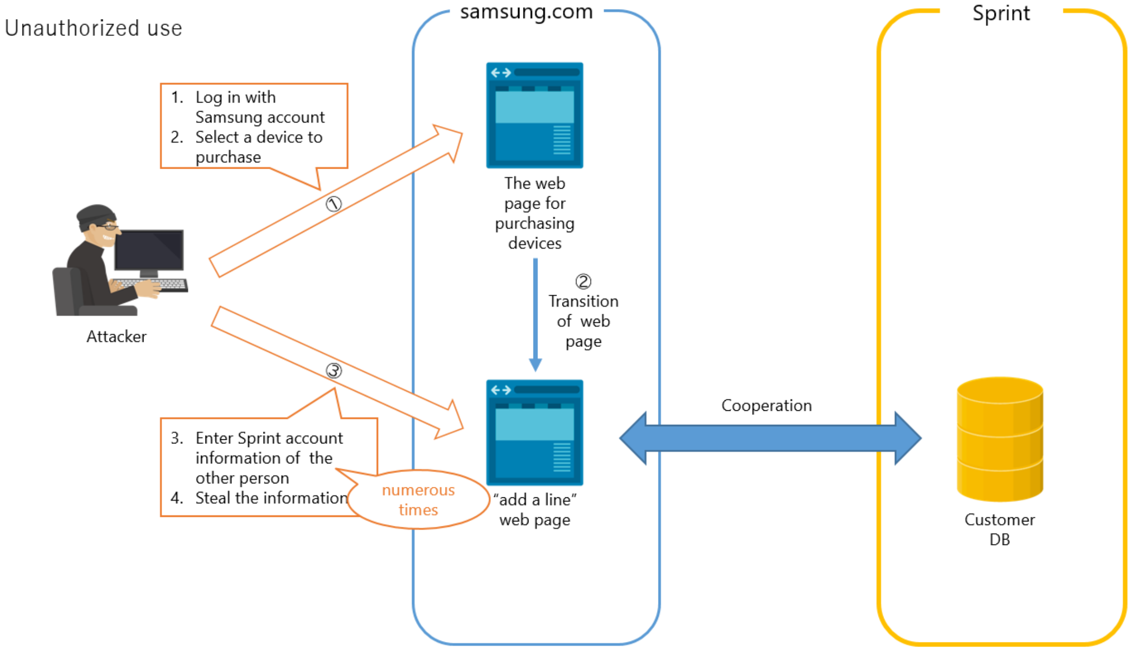

Unauthorized use
samsung.com
Sprint
1. Log in with Samsung account
2. Select a device to purchase
①
The web page for purchasing devices
Attacker
② Transition of web page
③
3. Enter Sprint account information of the other person
4. Steal the information
numerous times
“add a line” web page
Cooperation
Customer DB

Figure 2： Flow diagram of access in the case of unauthorized use

## Flow of Access in the Case of Unauthorized Use

① Access to the web page for purchasing devices

1. Attackers log in "samsung.com" with Samsung account that they already prepared
2. Select a device on the web page of samsung.com for purchasing devices

② Make a transition from the web page for purchasing devices to "add a line" web page

③ Access to add a line web page after taking over the state of login samsung.com

3. Enter authentication information of other people's Sprint account by a Brute-force attack.

④ When the authentication is successful, the information is shared between samsung.com and Sprint. Linked the purchased device and the new line contract

4. Attackers can see the information of its line contract
5. Repeat 3.and 4. over and over, and steal Sprint account information (ID and password)

Usually, attackers attack the organization whose security measures is optimistic, which connects with the target organization implemented security measures on supply chain and act as a stepping stone to success of attack , in order to attack the said target and then make a success of the attack .
However, for the preceding example, both organizations are not without enhancement of security measures. As it is generally known, the login page of the web system openly available on Internet must be implemented security measures against unauthorized access such as a Brute-force attack, etc. It seems that both Samsung.com and Sprint implement monitoring for unauthorized access to login page of their own system on a trial basis and unauthorized access measures such as lockout in case of consecutive login failure, etc. Even though organizations fulfill security measures each other, for some parts of connecting each system and business collaboration between different organizations, it would appear that many cases where the perimeter and scope of responsibility for security are ambiguous. [7] In this case, due to a blind spot of security measure that was the responsibility perimeter point, the said incident occurred. It would appear that both companies unexpected the need for measures against unauthorized access of points of which the group company of Samsung group's web system and Sprint's web system cooperates automatically. Risk analysis of this perimeter point was unsatisfied so that neither organizations realize that the Brute-force attack was possible from group companies of Samsung group's web system to Sprint's web system.

With regard to supply chain attack, even though organizations cooperate on supply chain implement risk analyses and security measures respectively, missing or leaking on somewhere may occur. The first method that prevents the said incident is to understand the whole supply chain and manage the perimeters of their responsibilities collectively and appropriately. For example, the methods are to be disclosed business procedures and contents of security measures to all clients and to be requested and implemented security measures. However, this method is only enabled to implement that its own organization is the most upstream on supply chain and all of organizations to marginal positions are perfectly disciplined. It is extremely difficult to fulfill all of them because under normal circumstances, fully understanding business procedures and systems of other organizations without own and managing all security measures cannot implement.

The second method is to be defined key role of implementation of security measures and the scope of responsibility between joint organizations in advance in order to implement security measures for each organization. The said method is to prevent missing and leaking security measures to clarify risks that may occur in advance and share them with the whole organization. However, there is the only way to trust joint organizations for the security measures of other organizations without own, required measures that are detection of attack and providing the bare minimum of information should implement in accordance with attack from joint organizations or provided data breach.

In fact, it is difficult to prevent supply chain attack completely so that it is necessary to reduce risks of the whole supply chain by cost-effective measures. There is currently no crucial method and measure to resolve this issue, therefore finding a best practice against supply chain attack is to be a common issue for the people concerned with security.

# 3. Data Breach

This chapter describes that data breach incidents identified during 2nd Quarter of FY2019. The trend through 4th Quarter of FY2018 to 1st Quarter of FY2019 has not been changed, data breach incidents such as web skimming and misconfiguration are easy to notice. The methods of attacks for web skimming have improved, and then the measures that infringe many web sites have been more effectively established. According to data breach incidents due to misconfiguration, the status, which a number of medical systems have published large amounts of information, has been identified.

## Web Skimming Improving Automatic Attack

Regarding the report of RISKIQ, attackers have automated the procedure that injects malicious codes for web skimming into EC sites by using programs. First, attackers scan EC sites using Amazon Simple Storage Server (hereinafter referred to as Amazon S3), find then the Amazon S3 which is misconfiguration. Second, if finding JavaScript files of EC sites into the Amazon S3 packet whose authority setting is misconfigured, attackers inject malicious codes for web skimming into the sites. Programs automatically repeat this procedure; attackers can inject malicious codes for web skimming into many EC sites in a short time. [8]
With regard to the survey of Sanguine Security, the large-scale web skimming campaign that infringed EC sites occurred on July 5, 2019. Malicious codes were injected on more than 960 web sites in a short time that is within 24 hours at this campaign. It is analyzed that attackers set up web skimming by using programs automated. [9]

## Data Breach due to Misconfiguration

Many data breach incidents have been reported during 2nd quarter of FY2019 continuously. There were many cases where classified information in database exposed to third parties due to misconfiguration of the database, as well as misconfiguration of other than database. Misconfiguration of firewall caused the incident that leaked personal information for 106 million people from the large financial company "Capital One" in July 2019. In addition, according to the survey of Greenbone Networks, approximately 2,300 of medical image management systems published medical images on Internet were found due to misconfiguration of those servers. Consequently, 400 million images were exposed.

## Data Breach Incidents

Table 2 below lists data breach incidents that occurred in 2nd quarter of FY2019.

Table 2 : Data breach incidents（2nd Quarter of FY2019）

| Date | Target Organizations | Cause | Summary |
|---|---|---|---|
| 7/1 | ORVIBO | Misconfiguration | The database including more than 2 billion of classified information was discovered to be exposed in two weeks **[10]** |
| 7/1 | Chinese Public Security Authority | Misconfiguration | The database including more than 90 million of personal information was discovered to be exposed **[11]** |
| 7/5 | Many e-commerce stores | Web skimming | The attack group "Magecart" infringed 962 of e-commerce stores by automation of malicious script injecting **[9]** |
| 7/8 | Fieldwork | Misconfiguration | The log data for 30 days (26GB) including information such as personal information, credit card information, and automatic log-in link, etc. was discovered to be exposed **[12]** |
| 7/30 | Capital One | Misconfiguration<br>Unauthorized access | Personal information for 106 million people leaked due to unauthorized access. Misconfiguration of firewall was exploited **[13]** |
| 8/19 | Option Way | Misconfiguration | Researcher of vpnMentor identified that the information of the database on the flight tickets booking site was available to access. 100GB of personal information was available to access **[14]** |
| 8/19 | DealerLeads | Misconfiguration | The database stored 198 million of customer information of purchasing cars was discovered to be exposed **[15]** |
| 9/4 | Facebook | Misconfiguration | 419 million of telephone numbers linked Facebook account were discovered on the server unprotected passwords **[16]** |
| 9/11 | Lion Air Group | Unauthorized access | 35 million of personal information was leaked due to unauthorized access of a contractor's staff **[17] [18]** |
| 9/16 | Many medical systems | Misconfiguration | The survey of Greenbone Networks identified that 2,300 of medical image management systems exposed 400 million medical images **[19]** |

## Conclusion

This chapter featured data breach relating to misconfiguration including automated web skimming. Setting systems appropriately is required to prevent data breach in advance. It is also important to check vulnerabilities of software and hardware. The point that attackers exploit breach of security has never changed to infringe systems. By automated attack program, attackers search systems left misconfigurations and vulnerabilities on Internet 24/7. Therefore, from the moment of disclosure of vulnerability information and occurring misconfiguration, taking time that discovers and attacks them becomes very short. The experiment result shows that an attack performed within about 10 minutes from occurring misconfigurations. There is a possibility that inadequately managed systems will be compromised in a short time more than expected. It is vital to prevent unauthorized access and data breach in advance based on prevention of misconfiguration and implementation of security patch promptly.

# 4. Vulnerability

## 4.1. Vulnerabilities of Some SSL/VPN Products

On September 6, 2019, JPCERT/CC published "Reminder related to vulnerabilities of some SSL/VPN products". [20] Concerned products and vulnerabilities are as follows.

- CVE-2019-1579 ：PAN-OS（Palo Alto Networks）
- CVE-2019-11510：Pulse Connect Secure, Pulse Policy Secure（Pulse Secure）
- CVE-2018-13379：FortiOS（Fortinet）

Some of products as above mentioned, if combined with other vulnerabilities, there is the vulnerability that can execute arbitrary code, it is therefore serious for all the three products. Those vulnerabilities have been commonly recognized among security specialists and attackers after disclosed in August 2019. From late August, scans of vulnerabilities and attacks against SSL/VPN products taken by attackers have become active.

DEVCORE published vulnerabilities of some SSL/VPN products and methods of attacks against them as above mentioned at "black hat USA 2019" held in August 2019. [21] SSL/VPN product is connecting users to an internal network safely via the Internet without physical dedicated lines, etc. If SSL/VPN products have a problem, attackers will be able to connect to the internal network from the Internet. The highest safety is therefore required for SSL/VPN products. According to the publication of DEVCORE, a number of companies have adopted SSL/VPN products, but the shares of them are concentrated in products of a few venders. Therefore, even though only one product has a vulnerability, the rate of the impact on systems using SSL/VPN will increase.

BAD PACKETS detected numerous scans against vulnerabilities of Pulse Secure products (CVE-2019-11510) in late August 2019. [22] Regarding the result of survey, as of August 24, 2019, Pulse Secure products unfixed their vulnerabilities, which were total 14,528, discovered on the Internet.

SSL/VPN products of Fortinet and Pulse Secure, there were a few vulnerabilities reported so far, it seems that many users did not often check the security patch. [21] Therefore, they discovered the vulnerabilities and security patch as mentioned above too late, and an attacker might have attacked them. The person in charge of information security requires careful attention to information of vulnerabilities and security patch for network devices like SSL/VPN products that protect Internet connection perimeter. Although information for vulnerabilities and security patch is provided rarely, do not cut corners on check of the information.

## 4.2. Other Exploited Vulnerabilities

Some vulnerabilities exploited in 2nd quarter of FY2019 are listed Table 3 as below. Except as vulnerabilities relating to "Vulnerabilities of Some SSL/VPN Products".

Table 3 : Exploited Vulnerabilities（2nd quarter of FY2019）

| Vulnerability No. | Target products | Summary |
|---|---|---|
| CVE-2019-9082<br>CVE-2019-3396<br>CVE-2018-7600, etc. | ThinkPHP<br>Atlassian Confluence<br>Drupal | On July 2, 2019, F5 reported that malware "Golang" has exploited some vulnerabilities of Linux server and spread mining malware on its own blog. [23] |
| CVE-2017-11774 | Outlook | On July 3, 2019, United States Cyber Command warned about cyberattacks against the government's network exploiting vulnerabilities disclosed in July 2017. [24] |
| CVE-2019-1132 | Windows | In June 2019, the attack group "Buhtrap" implemented zero-day attack exploited vulnerabilities against government agencies. [25] [26] Information of the vulnerabilities was published on July 9, 2019. |
| CVE-2019-8978 | Ellucian Banner System | United States Department of Education warned about attacks targeted ERP for universities on July 7, 2019. 62 universities were impacted. [27] |
| CVE-2019-0708<br>BlueKeep | Windows | On July 23, 2019, exploit code was added in the tool "CANVAS". [28] On July 24, 2019, the function scanning vulnerabilities was added in malware "WatchBog". [29] On September 6, 2019, exploit module was added in the tool "Metasploit". [30] |
| Some vulnerabilities | WordPress<br>Plug-in | Wordfence reported attacks exploiting vulnerabilities of some WordPress plug-in. [31] [32] |
| No CVE number | Apple iOS | Google discovered the Web site that tries to hack by exploiting undisclosed vulnerabilities. Apple announced the attacks were limited. [33] [34] |
| No CVE number | LINE | LINE reported that they fixed the vulnerabilities on the same day after reported vulnerabilities on August 31, 2019. Attacks through August 30 to 31 were observed. [35] |
| No CVE number<br>Simjacker | SIM card | On September 12, 2019, Adaptive Mobile Security published "Simjacker" that is the attack exploiting vulnerabilities of SIM cards. The exploitations have occurred from two years ago. [36] |

| Vulnerability No. | Target products | Summary |
|---|---|---|
| CVE-2019-1367 | Internet Explorer | On September 23, 2019, Microsoft fixed vulnerabilities on security updating programs that was not periodic. One of the IE vulnerabilities was to be checked the prerelease exploitation of vulnerability. [37] |

# 5. Malware/Ransomware

## Ransomware Incidents Exploding in the USA

In 2nd Quarter of FY2019, Ransomware incidents continue to explode in the USA from 1st Quarter of FY2019. Local public authorities are continuously targeted, as well as schools and medical institutions. During 2nd Quarter of FY2019, incidents caused by Ransomware in the USA are listed Table 4 as below.

Table 4 : Incidents caused by Ransomware in the USA

| Date | Target | Summary |
|---|---|---|
| 7/1 | Georgia State<br>The court | Shut down the network of the court due to Ransomware attacks. The Ransomware ”Ryuk” was used. [38] |
| 7/5 | Massachusetts State<br>New Bedford City | 158 computers were encrypted due to the incident of variant of Ransomware “Ryuk”. There was a ransom demand of $5.3 million but The city declined it. [39] |
| 7/6 | Indiana State<br>La Porte County | Paid $130 thousand in ransom due to Ransomware attacks “Ryuk”. Owing to early detection, infection computers were minimized only for 7% of the whole network, however domain controllers were included, this county’s system was shut down. [40] |
| 7/10 | New York State<br>Monroe College | Shut down the system due to Ransomware attacks. There was a ransom demand of 2 million worth of bitcoins. Whether Paying the ransom is unknown. [41] |
| 7/16 | Indiana State<br>Vigo County | Associated Press announced that used Ransomware could been unidentified yet and the policy that they declined the ransom demand. [42] |
| 7/27 | Georgia State<br>Public Safety Department | Georgia State Patrol, Georgia Capitol Police, and Georgia Motor Carrier Compliance Division were affected by Ransomware attacks. Although all of IT systems were shut down, telephones, etc. were substituted for the systems, there was no adverse impact for their businesses. [43] |
| 7/30 | Alabama State<br>Huston County<br>The school | Due to malware attacks, The school deferred the day of open school twice a week. Security specialists infer that the school took a long time to fix the system because of Ransomware attacks. [44] |
| 8/16 | Texas State<br>Government agencies | Ransomware attacked 23 government agencies at the same time. Almost of all impacted systems were the ones for small amount of local public authorities. They all have their policies that do not pay ransom. [45] |

| Date | Target | Summary |
|---|---|---|
| 8/27 | Dentists | Cloud service for dental diagnosis in the USA "DDS Safe", Digital Dental Record and PerCSoft provided jointly, was attacked by Ransomware. There were impacts that 400 dentists could not access patient's information, etc. [46] |
| 9/4 | Connecticut State Wolcott public school | School officials could not use Internet and the mail system due to Ransomware attacks. Ransomware attacked Wolcott public school in June 2019. They were affected twice. [47] |
| 9/20 | Wyoming State Campbell county memorial hospital | The operation of the hospital was affected according to Ransomware attacks. Some surgeries and examinations were canceled and Campbell county memorial hospital announced its policy that some patients were transferred from this hospital to others as appropriate. [48] |

Some organizations in the USA have announced their statements and policies according to Ransomware incidents. On July 10, 2019, US Conference of Mayors adopted a resolution not to pay ransoms to hackers. [49] On July 30, 2019, CISA[1], MS-ISAC[2], NGA[3], and NASCIO[4] announced the joint statement encouraging people to implement measures that are "Backup of systems", "Trainings against cyberattacks for staff members", and "Review of incident response plan when attacks occur". [50] On August 21, 2019, CISA published procedures integrated "Implementations for protection of organizations", "Implementations when infected", and "Implementations for protection of environment in the future", etc. [51] In addition, according to the survey that Morning Consult and IBM jointly performed, 63% of US civilians desire using tax money for recovery costs rather than using it for paying ransoms, and 90% of them agree on increase in federal budget to protect functions of cities ceased by cyberattacks. [52]

[1] Cybersecurity and Infrastructure Security Agency

[2] Multi-State Information Sharing and Analysis Center

[3] National Geospatial-Intelligence Agency

[4] National Association of State Chief Information Officers

## Emotet Spread Mail Leading to Ransomware Attacks

As an example of a cyberattack leading to Ransomware incidents, there is the Emotet spread mail. [53] First of all, attackers spread the malware "Emotet" to the people belonging to the target organization by exploiting email. Computers infected Emotet infect the malware "TrickBot" due to the function of Emotet that distributes malwares. The main function of TrickBot is to be abstraction of information. TrickBot abstracts highly confidential information of target organizations. If being able to acquire important information to demand a ransom, TrickBot will download and implement the Ransomware. This method of attack, which uses Emotet for the function of malware distribution, TrickBot for the function of abstraction of information, and Ryuk for Ransomware that demands a ransom, called "Triple Threat" that combines three types of malwares. The procedure of Triple Threat attacks is described Figure 3 as below. An actual incident caused by Triple Threat, at state of Florida in the USA was attacked in June 2019, consequently $460 thousand were paid for attackers. [54]

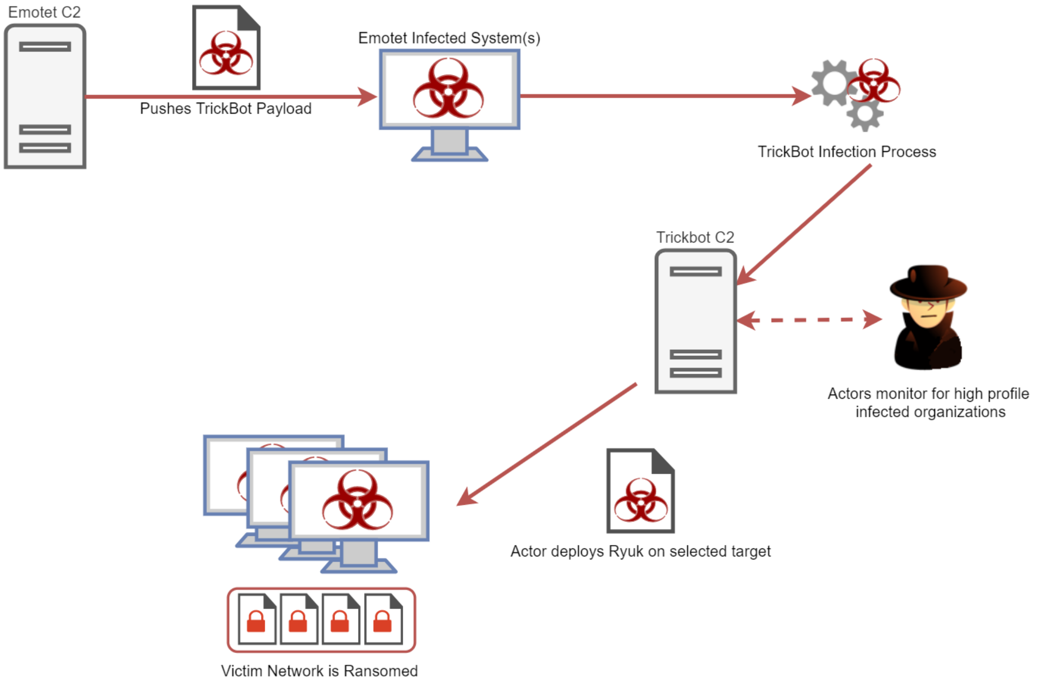

Emotet C2
Pushes TrickBot Payload
Emotet Infected System(s)
TrickBot Infection Process
Trickbot C2
Actors monitor for high profile infected organizations
Actor deploys Ryuk on selected target
Victim Network is Ransomed

Figure 3 : Procedure of "Triple Threat" attacks
(Reprinted from CYBEREASON official blog [53])

## Trend of Emotet

As mentioned in the report of 1st Quarter of FY2019, Emotet is a malware that continues to evolve over 5 years. According to the survey of Cofense, Emotet ceased its actions most of months in June and July after active actions in May. [55] However, regarding the survey of MalwareTech, an active C&C server was newly discovered in August 21, 2019, Activities of Emotet were observed in many regional hubs including Brazil, Mexico, Germany, Japan, and US. [56] Recently, Emotet mainly has spread by email and sophisticated attacks have been increasing. After 2nd Quarter of FY2019, numerous Emotet spread mails whose titles and texts are written in Japanese are observed in Japan.

Emotet is extremely jeopardous malware because it has the worm function that infects computers as much as possible, the function that spreads email for infection spread from infected computers to other organizations, and the function that distributes other malwares. For the reasons above mentioned, CISA reported that Emotet is one of the most destructive botnet they have ever seen in the warning published in July 2019. [57] Sophos described that Emotet attacks are much more jeopardous than WannaCry's in 2017 in the past report published. [58]

## Conclusions

From 1st Quarter of FY2019 to now 2nd Quarter of FY2019 continuously, Ransomware attacks have been concentrated in the USA, a number of incidents therefore have occurred. The main reason why attackers target local public authorities in the USA is that US is more likely to pay ransoms due to Ransomware attacks than other countries. In the future, Ransomware's targets could be changed because of impact of the resolution disagreed paying ransoms.

Lists that should implement right now, written in the warning CISA published in August 2019, describe the training using the latest incidents in addition to data backup and system update. Trainings are to be important measures to minimize Ransomware incidents and recover early. First, let us create procedures of measures by reference to reports that describe situations when infected Ransomware and details of incident responses and by expecting the case where the same incident occurs in own company. Second, let us check that the system can be correctly recovered in fact by using the procedures created. Finally, let us practice to minimize impact of incidents such as isolating infected machines and shutting down the network and to recover the system from data backup in order to get the business back to normal in the short time for case of emergency.

# 6. Outlook

In this section, we describe present trends and outlooks from incidents occurred in 2nd quarter of FY2019.  There are trends to perform automation, sophistication, functional addition, and change of target against existing methods of attacks. Care and attention are required because there are some cases that cannot prevent incidents by the same measures as before.

## Arise of Cyberattacks Methods Searching Misconfiguration Automatically

Attackers established methods to attack effectively services and systems that have misconfigurations. As mentioned in “3. Data Breach”, the automated web skimming infringed 960 web sites within 24 hours to scan misconfigurations of Amazon S3. It is possible to detect targets having misconfigurations for attacks all together to focus on targets for specific services like AWS rather than port scan. That is extremely precarious method in the present day when increasing accesses to public clouds and platforms. From 3rd quarter of FY2019, there is possibility that misconfigurations of popular public clouds and platforms will be targets all together. We recommend implementing configurations related to security such as access control appropriately when using those services and systems.

## Malware Distribution via Email

Email is still using for targeted malware distribution. This reason why is because email is the most useful communication tool business between different organizations so far. Although there are trends to increase companies using communication tools except email for business communication between different organizations, they are minority relative to organizations using email. It is difficult to discontinue using email completely under the current circumstances. Taking into account this feature, emails are appropriate to the method that deceive targets to pretend the person belonging to an external organization. For those reasons, it is predicted that cyberattacks exploiting email continue for a while longer. Especially, emails distributing malware cleverly try to deceive targets with a succession of method, therefore It would appear that the impacts may continue.

## Expanding Impacts of Ransomware Attacks

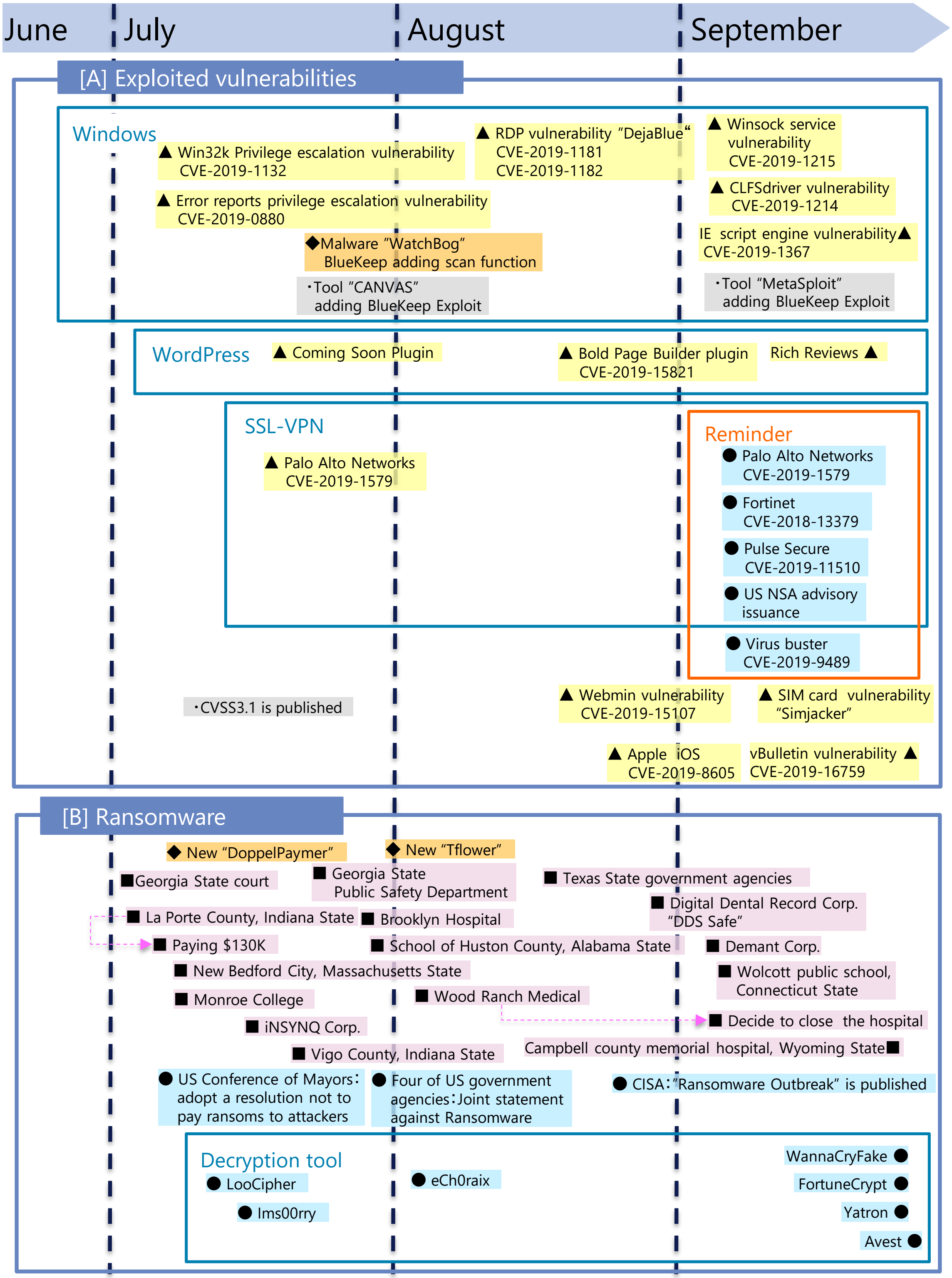
Nowadays, Ransomware attacks have concentrated in local public authorities in the USA. This reason why is because there is a possibility that US, which was more likely to pay ransoms due to Ransomware attacks than other countries, is targeted by the attacks. However, opinions that disagree paying ransoms have been increasing strongly due to a number of impacts In the USA. If US does not accept to pay ransoms easily as well as other countries, it would appear that targets might be changed. In addition, according to Ransomware attacks, if the attacks are successful and targets pay ransoms, attackers make massive money. However even if the attacks are successful but targets do not pay them, attackers make no money. Taking into account this feature, attackers focus on attacks to a large number of organizations at the same time rather than improving the success rate of the attack. From here onwards, on and after 3rd quarter of FY2019, it is expected that much more organizations will be affected according to Ransomware attacks at the same time. We recommend reviewing the status of measure for one’s own organization and policies relating to recovery and paying ransoms before impacts occur due to Ransomware attacks.

# 7. Timeline

*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



June July August September

[A] Exploited vulnerabilities

Windows

▲ Win32k Privilege escalation vulnerability CVE-2019-1132

▲ Error reports privilege escalation vulnerability CVE-2019-0880

◆Malware "WatchBog" BlueKeep adding scan function

・Tool "CANVAS" adding BlueKeep Exploit

▲ RDP vulnerability "DejaBlue" CVE-2019-1181 CVE-2019-1182

▲ Winsock service vulnerability CVE-2019-1215

▲ CLFSdriver vulnerability CVE-2019-1214

IE script engine vulnerability▲ CVE-2019-1367

・Tool "MetaSploit" adding BlueKeep Exploit

WordPress

▲ Coming Soon Plugin

▲ Bold Page Builder plugin CVE-2019-15821

Rich Reviews ▲

SSL-VPN

▲ Palo Alto Networks CVE-2019-1579

Reminder

● Palo Alto Networks CVE-2019-1579

● Fortinet CVE-2018-13379

● Pulse Secure CVE-2019-11510

● US NSA advisory issuance

● Virus buster CVE-2019-9489

・CVSS3.1 is published

▲ Webmin vulnerability CVE-2019-15107

▲ SIM card vulnerability "Simjacker"

▲ Apple iOS CVE-2019-8605

vBulletin vulnerability ▲ CVE-2019-16759

[B] Ransomware

◆ New "DoppelPaymer"

◆ New "Tflower"

■Georgia State court

■ Georgia State Public Safety Department

■ Texas State government agencies

■ Digital Dental Record Corp. "DDS Safe"

■ La Porte County, Indiana State

■ Paying $130K

■ Brooklyn Hospital

■ School of Huston County, Alabama State

■ Demant Corp.

■ New Bedford City, Massachusetts State

■ Wolcott public school, Connecticut State

■ Monroe College

■ Wood Ranch Medical

■ Decide to close the hospital

■ iNSYNQ Corp.

■ Vigo County, Indiana State

Campbell county memorial hospital, Wyoming State■

● US Conference of Mayors: adopt a resolution not to pay ransoms to attackers

● Four of US government agencies:Joint statement against Ransomware

● CISA:"Ransomware Outbreak" is published

Decryption tool

● LooCipher

● Ims00rry

● eCh0raix

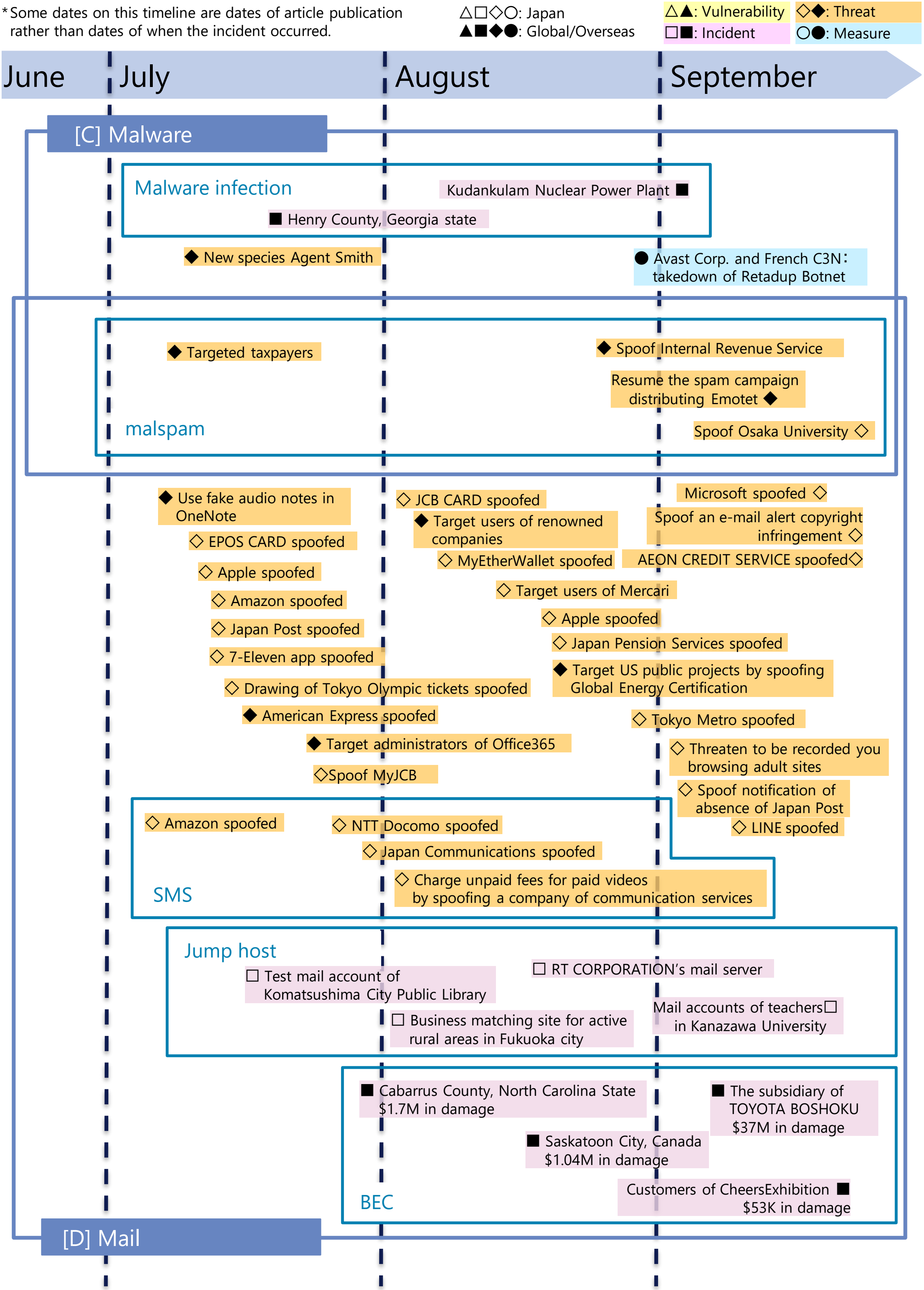
WannaCryFake ●

FortuneCrypt ●

Yatron ●

Avest ●

Timeline



*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure

June | July | August | September

[C] Malware

Malware infection

Kudankulam Nuclear Power Plant ■

■ Henry County, Georgia state

◆ New species Agent Smith

● Avast Corp. and French C3N：takedown of Retadup Botnet

malspam

◆ Targeted taxpayers

◆ Spoof Internal Revenue Service

Resume the spam campaign distributing Emotet ◆

Spoof Osaka University ◇

◆ Use fake audio notes in OneNote

◇ EPOS CARD spoofed

◇ Apple spoofed

◇ Amazon spoofed

◇ Japan Post spoofed

◇ 7-Eleven app spoofed

◇ Drawing of Tokyo Olympic tickets spoofed

◆ American Express spoofed

◆ Target administrators of Office365

◇Spoof MyJCB

◇ JCB CARD spoofed

◆ Target users of renowned companies

◇ MyEtherWallet spoofed

◇ Target users of Mercari

◇ Apple spoofed

◇ Japan Pension Services spoofed

◆ Target US public projects by spoofing Global Energy Certification

Microsoft spoofed ◇

Spoof an e-mail alert copyright infringement ◇

AEON CREDIT SERVICE spoofed◇

◇ Tokyo Metro spoofed

◇ Threaten to be recorded you browsing adult sites

◇ Spoof notification of absence of Japan Post

◇ LINE spoofed

SMS

◇ Amazon spoofed

◇ NTT Docomo spoofed

◇ Japan Communications spoofed

◇ Charge unpaid fees for paid videos by spoofing a company of communication services

Jump host

□ Test mail account of Komatsushima City Public Library

□ Business matching site for active rural areas in Fukuoka city

□ RT CORPORATION’s mail server

Mail accounts of teachers□ in Kanazawa University

BEC

■ Cabarrus County, North Carolina State $1.7M in damage

■ Saskatoon City, Canada $1.04M in damage

■ The subsidiary of TOYOTA BOSHOKU $37M in damage

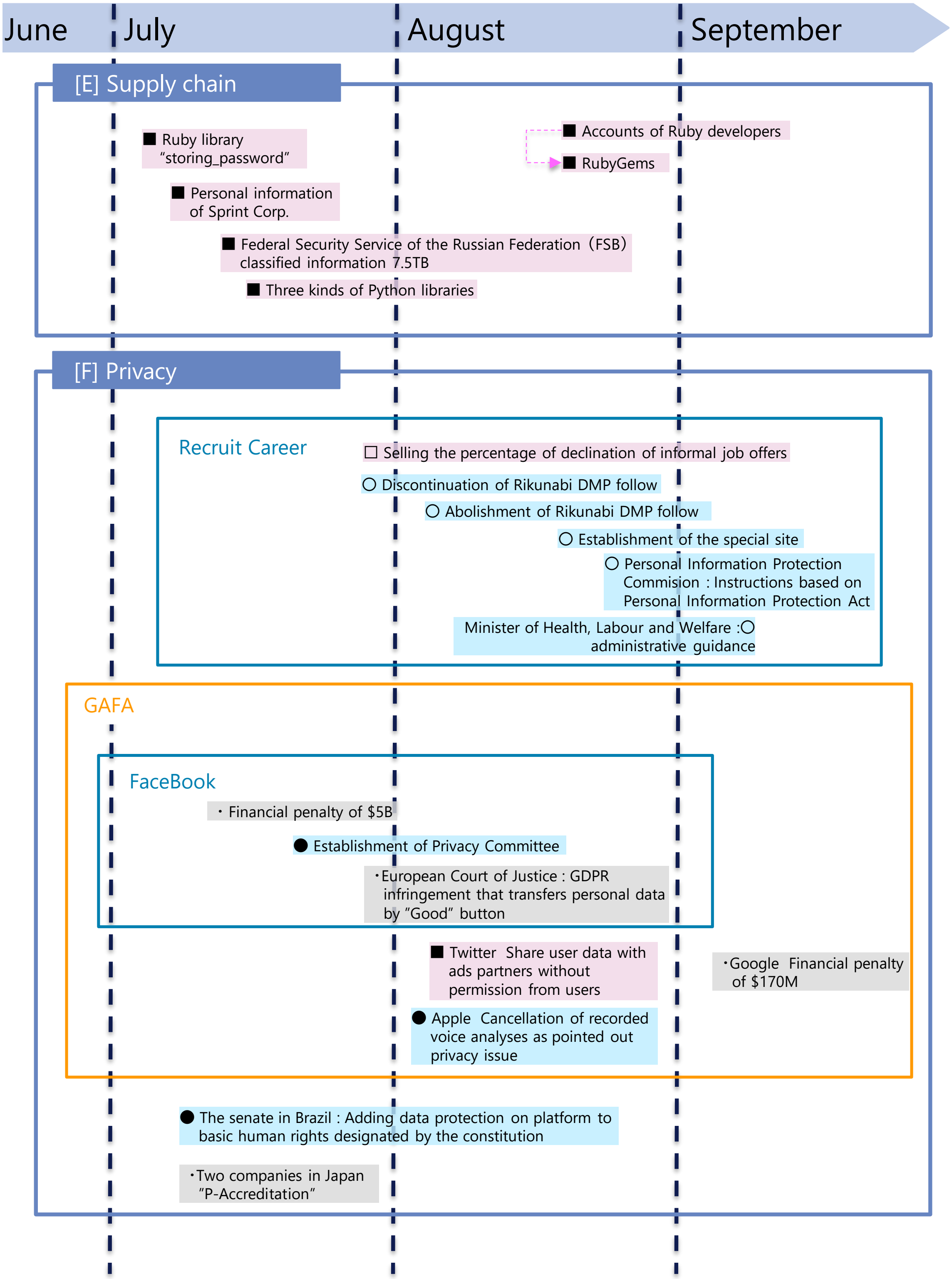
Customers of CheersExhibition ■ $53K in damage

[D] Mail

*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



June | July | August | September

[E] Supply chain

■ Ruby library "storing_password"

■ Personal information of Sprint Corp.

■ Federal Security Service of the Russian Federation（FSB） classified information 7.5TB

■ Three kinds of Python libraries

■ Accounts of Ruby developers

■ RubyGems

[F] Privacy

Recruit Career

□ Selling the percentage of declination of informal job offers

○ Discontinuation of Rikunabi DMP follow

○ Abolishment of Rikunabi DMP follow

○ Establishment of the special site

○ Personal Information Protection Commision : Instructions based on Personal Information Protection Act

Minister of Health, Labour and Welfare :○ administrative guidance

GAFA

FaceBook

・Financial penalty of $5B

● Establishment of Privacy Committee

・European Court of Justice : GDPR infringement that transfers personal data by "Good" button

■ Twitter Share user data with ads partners without permission from users

● Apple Cancellation of recorded voice analyses as pointed out privacy issue

・Google Financial penalty of $170M

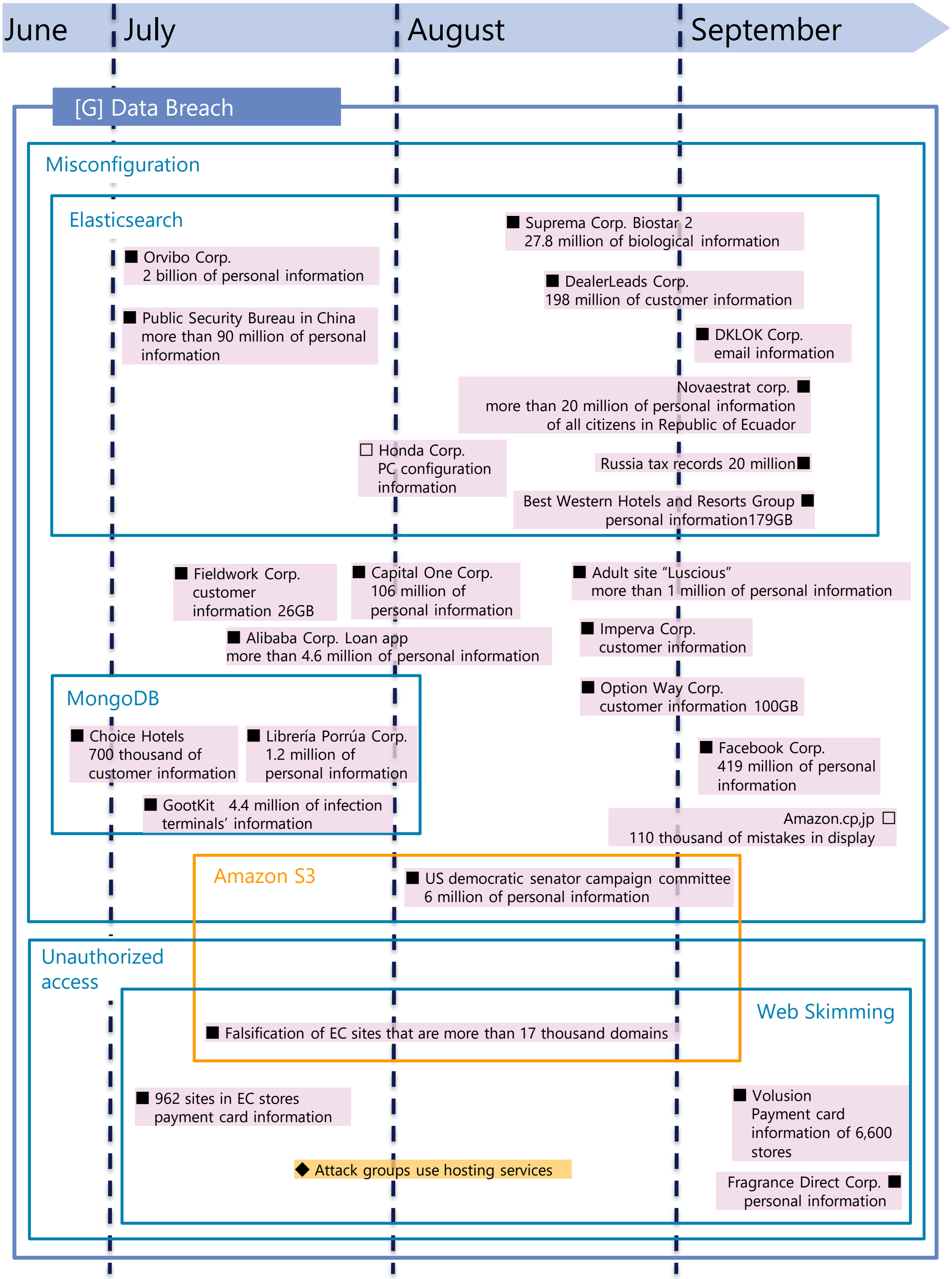
● The senate in Brazil : Adding data protection on platform to basic human rights designated by the constitution

・Two companies in Japan "P-Accreditation"

*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



June | July | August | September

[G] Data Breach

Misconfiguration

Elasticsearch

■ Orvibo Corp.
2 billion of personal information

■ Public Security Bureau in China
more than 90 million of personal information

■ Suprema Corp. Biostar 2
27.8 million of biological information

■ DealerLeads Corp.
198 million of customer information

■ DKLOK Corp.
email information

Novaestrat corp. ■
more than 20 million of personal information
of all citizens in Republic of Ecuador

□ Honda Corp.
PC configuration information

Russia tax records 20 million■

Best Western Hotels and Resorts Group ■
personal information179GB

■ Fieldwork Corp.
customer information 26GB

■ Capital One Corp.
106 million of personal information

■ Alibaba Corp. Loan app
more than 4.6 million of personal information

■ Adult site "Luscious"
more than 1 million of personal information

■ Imperva Corp.
customer information

■ Option Way Corp.
customer information 100GB

■ Facebook Corp.
419 million of personal information

Amazon.cp.jp □
110 thousand of mistakes in display

MongoDB

■ Choice Hotels
700 thousand of customer information

■ Librería Porrúa Corp.
1.2 million of personal information

■ GootKit 4.4 million of infection terminals' information

Amazon S3

■ US democratic senator campaign committee
6 million of personal information

Unauthorized access

Web Skimming

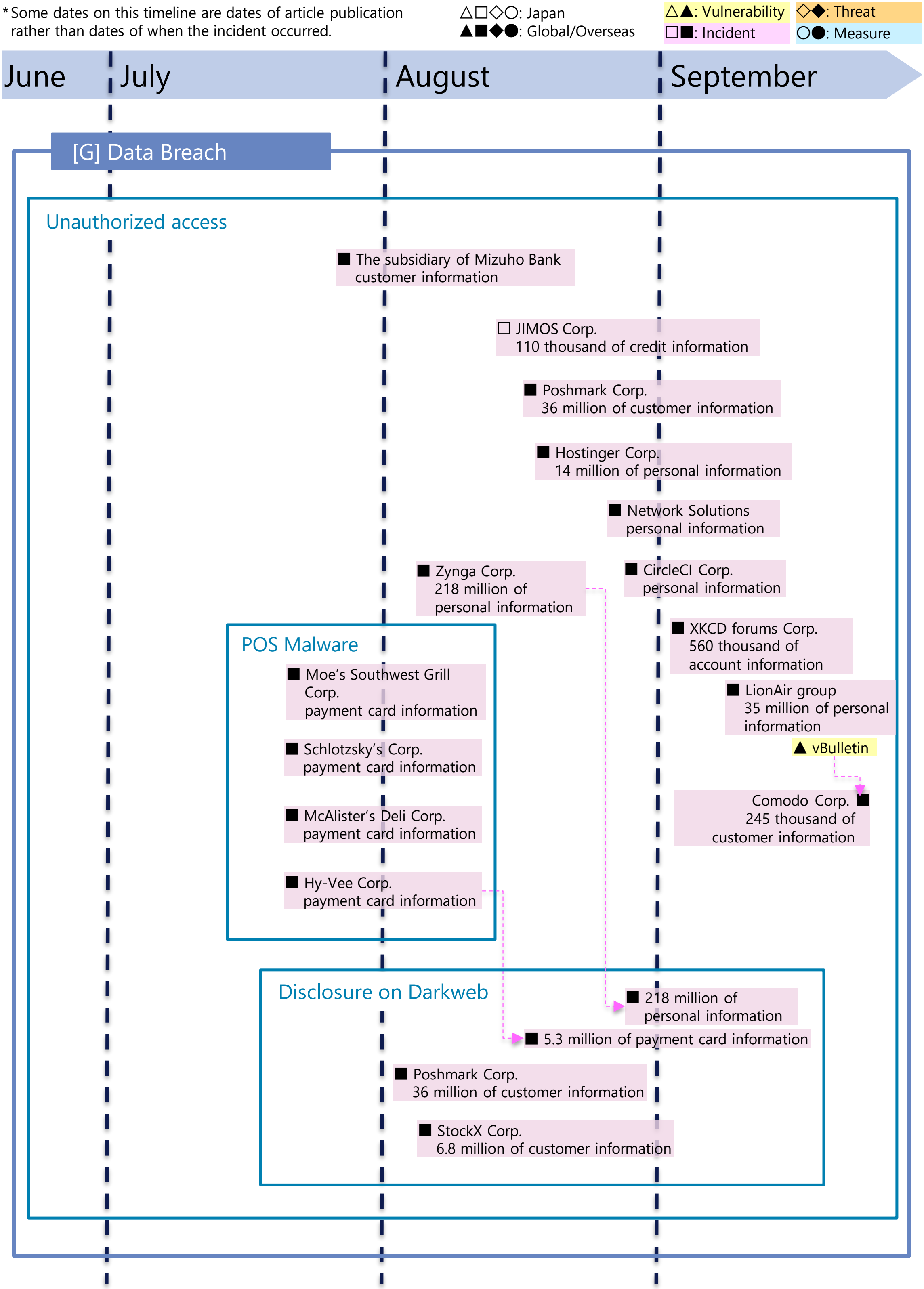
■ Falsification of EC sites that are more than 17 thousand domains

■ 962 sites in EC stores
payment card information

◆ Attack groups use hosting services

■ Volusion
Payment card information of 6,600 stores

Fragrance Direct Corp. ■
personal information



*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure

June | July | August | September

[G] Data Breach

Unauthorized access

■ The subsidiary of Mizuho Bank customer information

□ JIMOS Corp. 110 thousand of credit information

■ Poshmark Corp. 36 million of customer information

■ Hostinger Corp. 14 million of personal information

■ Network Solutions personal information

■ Zynga Corp. 218 million of personal information

■ CircleCI Corp. personal information

■ XKCD forums Corp. 560 thousand of account information

■ LionAir group 35 million of personal information

▲ vBulletin

Comodo Corp. ■ 245 thousand of customer information

POS Malware

■ Moe's Southwest Grill Corp. payment card information

■ Schlotzsky's Corp. payment card information

■ McAlister's Deli Corp. payment card information

■ Hy-Vee Corp. payment card information

Disclosure on Darkweb

■ 218 million of personal information

■ 5.3 million of payment card information

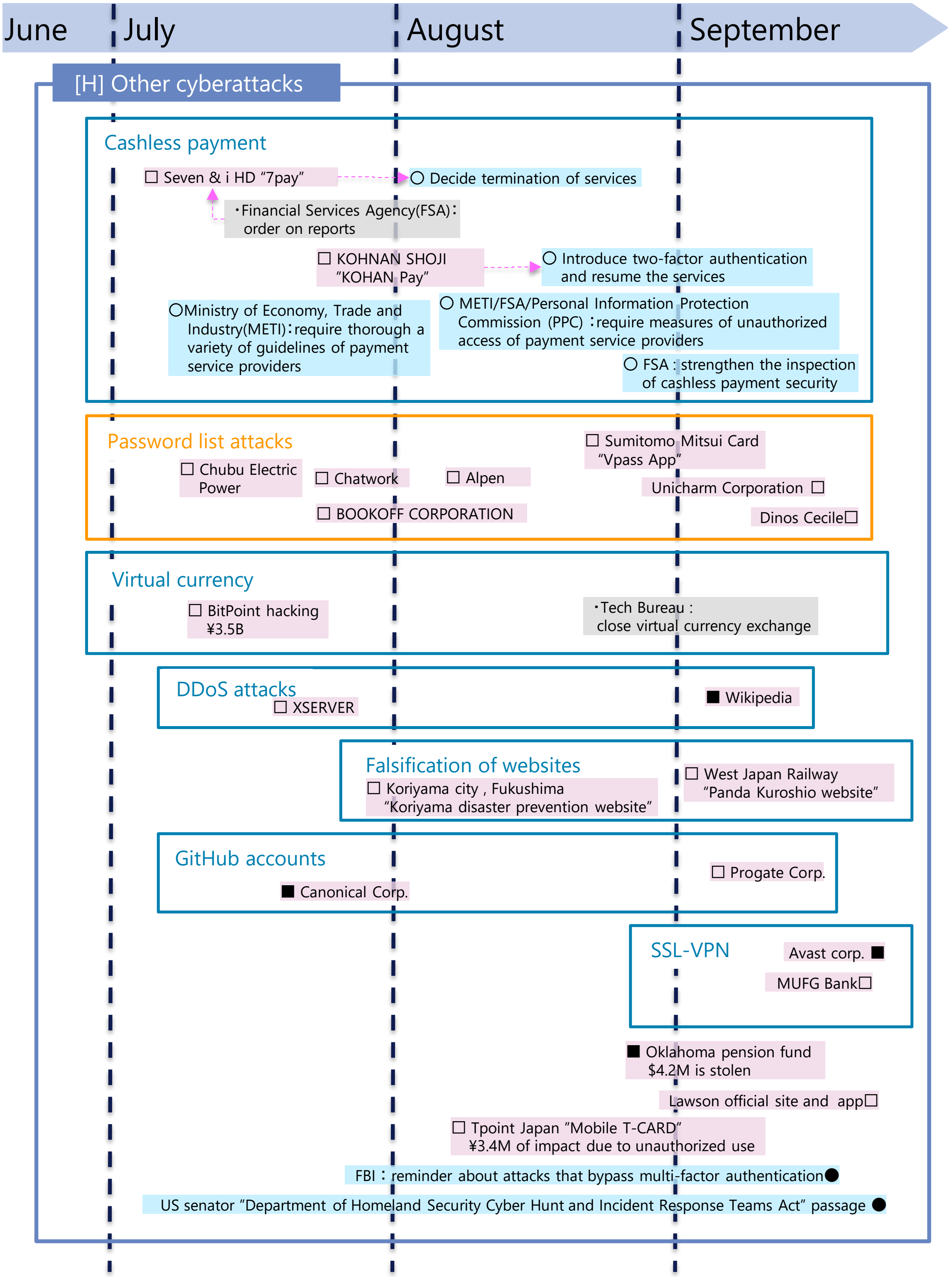
■ Poshmark Corp. 36 million of customer information

■ StockX Corp. 6.8 million of customer information

*Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



[H] Other cyberattacks

Cashless payment

□ Seven & i HD "7pay"

○ Decide termination of services

・Financial Services Agency(FSA)：order on reports

□ KOHNAN SHOJI "KOHAN Pay"

○ Introduce two-factor authentication and resume the services

○Ministry of Economy, Trade and Industry(METI)：require thorough a variety of guidelines of payment service providers

○ METI/FSA/Personal Information Protection Commission (PPC) ：require measures of unauthorized access of payment service providers

○ FSA : strengthen the inspection of cashless payment security

Password list attacks

□ Chubu Electric Power

□ Chatwork

□ Alpen

□ BOOKOFF CORPORATION

□ Sumitomo Mitsui Card "Vpass App"

Unicharm Corporation □

Dinos Cecile□

Virtual currency

□ BitPoint hacking ¥3.5B

・Tech Bureau : close virtual currency exchange

DDoS attacks

□ XSERVER

■ Wikipedia

Falsification of websites

□ Koriyama city , Fukushima "Koriyama disaster prevention website"

□ West Japan Railway "Panda Kuroshio website"

GitHub accounts

■ Canonical Corp.

□ Progate Corp.

SSL-VPN

Avast corp. ■

MUFG Bank□

■ Oklahoma pension fund $4.2M is stolen

Lawson official site and app□

□ Tpoint Japan "Mobile T-CARD" ¥3.4M of impact due to unauthorized use

FBI：reminder about attacks that bypass multi-factor authentication●

US senator "Department of Homeland Security Cyber Hunt and Incident Response Teams Act" passage ●

# References

[1] KADOKAWA ASCII Research Laboratories, Inc, "2018年はどんなセキュリティ脅威が？9社予測まとめ《前編》," 5 1 2018. [Online]. Available: https://ascii.jp/elem/000/001/611/1611970/.

[2] 尚. 大谷, 義. 小林, 眞. 大石 and 大. 山下, "グローバルセキュリティ動向四半期レポート 2018年度第4四半期," 株式会社NTTデータ, 30 5 2019. [Online]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_4q_securityreport.pdf.

[3] C. Cimpanu, "Hackers breach FSB contractor, expose Tor deanonymization project and more," CBS Interactive., 20 7 2019. [Online]. Available: https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/.

[4] C. Cimpanu, "Sprint says hackers breached customer accounts via Samsung website," CBS Interactive., 16 7 2019. [Online]. Available: https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/.

[5] C. Cimpanu, "Sprint breach notification (Samsung.com)," Scribd Inc., [Online]. Available: https://www.scribd.com/document/417811440/Sprint-breach-notification-Samsung-com. [Accessed 12 11 2019].

[6] Symantec Security Response Attack Investigation Team, "Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks," Broadcom., 18 9 2019. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

[7] "「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について," 独立行政法人　情報処理推進機構, 19 4 2019. [Online]. Available: https://www.ipa.go.jp/security/fy30/reports/scrm/index.html.

[8] RISKIQ, "Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets," 10 7 2019. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/.

[9] BleepingComputer, "Automated Magecart Campaign Hits Over 960 Breached Stores," 5 7 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/automated-magecart-campaign-hits-over-960-breached-stores/.

[10] ZDNet, "Smart home maker leaks customer data, device passwords," 1 7 2019. [Online]. Available: https://www.zdnet.com/article/smart-home-maker-leaks-customer-data-device-passwords/.

[11] Bleeping Computer, "Over 90 Million Records Leaked by Chinese Public Security Department," 8 7 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-90-million-records-leaked-by-chinese-public-security-department/.

[12] vpnMentor, "Report: Fieldwork Software Leaks Sensitive Customer Data," 8 7 2019. [Online]. Available: https://www.vpnmentor.com/blog/report-fieldwork-leak/.

[13] Capital One, "Information on the Capital One Cyber Incident," 28 7 2019. [Online]. Available: https://www.capitalone.com/facts2019/.

[14] vpnMentor, "Report: Flight Booking Platform Exposes Customer Data," 2 9 2019. [Online]. Available: https://www.vpnmentor.com/blog/report-option-way-leak/.

[15] Security Discovery, "Auto Dealer Leads Network Exposed 198 Million Records Online," 11 9 2019. [Online]. Available: https://securitydiscovery.com/dealer-leads/.

[16] TechCrunch, "A huge database of Facebook users' phone numbers found online," 4 9 2019. [Online]. Available: https://www.businessinsider.jp/post-198159.

[17] ZDNet, "AWS servers 'secure' following Malindo Air data breach," 20 9 2019. [Online]. Available: https://www.zdnet.com/article/aws-says-servers-secure-following-malindo-air-data-breach/.

[18] The Jakarta Post, "Lion Air data stolen, leaked by ex-GoQuo employees," 24 9 2019. [Online]. Available: https://www.thejakartapost.com/news/2019/09/24/lion-air-data-stolen-leaked-by-ex-goquo-employees.html.

[19] Grreenbone Networks, "Information Security Report," 16 9 2019. [Online]. Available: https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf.

[20] JPCERT/CC, "複数の SSL VPN 製品の脆弱性に関する注意喚起," 6 9 2019. [Online]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[21] DEVCORE, "Infiltrating Corporate Intranet," 7 8 2019. [Online]. Available: https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf.

[22] BAD PACKETS, 24 8 2019. [Online]. Available: https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/.

[23] F5, "New Golang Malware is Spreading via Multiple Exploits to Mine Monero," 2 7 2019. [Online]. Available: https://www.f5.com/labs/articles/threat-intelligence/new-golang-malware-is-spreading-via-multiple-exploits-to-mine-mo.

[24] Security Affairs, "US Cyber Command warns of Iran-linked hackers exploiting CVE-2017-11774 Outlook flaw," 3 7 2019. [Online]. Available: https://securityaffairs.co/wordpress/87895/breaking-news/cve-2017-11774-apt33-attacks.html.

[25] Microsoft, "CVE-2019-1132 | Win32k Elevation of Privilege Vulnerability," 9 7 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1132.

[26] Bleeping Computer, "Windows Zero-Day Used by Buhtrap Group For Cyber-Espionage," 11 7 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/windows-zero-day-used-by-buhtrap-group-for-cyber-espionage/.

[27] Federal Student Aid, "TECHNOLOGY SECURITY ALERT – Exploitation of Ellucian Banner System Vulnerability," 17 7 2019. [Online]. Available: https://ifap.ed.gov/eannouncements/071719ITSecurAlertExploitationEllucianBannerSysVulnerability.html.

[28] Bleeping Computer, "BlueKeep RCE Exploit Module Added to Penetration Testing Tool," 25 7 2019. [Online]. Available: bleepingcomputer.com/news/security/bluekeep-rce-exploit-module-added-to-penetration-testing-tool/.

[29] INTEZER, "Watching the WatchBog: New BlueKeep Scanner and Linux Exploits," 19 7 2019. [Online]. Available: https://www.intezer.com/blog-watching-the-watchbog-new-bluekeep-scanner-and-linux-exploits/.

[30] ZDNet, "Metasploit team releases BlueKeep exploit," 6 9 2019. [Online]. Available: https://www.zdnet.com/article/metasploit-team-releases-bluekeep-exploit/.

[31] Wordfence, "Recent WordPress Vulnerabilities Targeted by Malvertising Campaign," 22 7 2019. [Online]. Available: https://www.wordfence.com/blog/2019/07/recent-wordpress-vulnerabilities-targeted-by-malvertising-campaign/.

[32] Wordfence, "Ongoing Malvertising Campaign Evolves, Adds Backdoors and Targets New Plugins," 30 8 2019. [Online]. Available: https://www.wordfence.com/blog/2019/08/ongoing-malvertising-campaign-continues-exploiting-new-vulnerabilities/.

[33] Google Project Zero, "A very deep dive into iOS Exploit chains found in the wild," 29 8 2019. [Online]. Available: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html.

[34] Apple, "A message about iOS security," 6 9 2019. [Online]. Available: https://www.apple.com/newsroom/2019/09/a-message-about-ios-security/.

[35] LINE, "LINEアカウントのプロフィール画像を変更可能な脆弱性の修正のお知らせ," 2 9 2019. [Online]. Available: https://linecorp.com/ja/security/article/224.

[36] AdaptiveMobile Security, "Simjacker – Next Generation Spying Over Mobile," 12 9 2019. [Online]. Available: https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile.

[37] Microsoft, "CVE-2019-1367 | Scripting Engine Memory Corruption Vulnerability," 23 9 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367.

[38] SOPHOS, "Georgia’s court system hit by ransomware," 3 7 2019. [Online]. Available: https://nakedsecurity.sophos.com/2019/07/03/georgias-court-system-hit-by-ransomware/.

[39] New　Bedford, "MAYOR DISCUSSES IMPACT OF RANSOMWARE ATTACK ON NEW BEDFORD’S COMPUTER SYSTEM," 5 7 2019. [Online]. Available: https://www.newbedford-ma.gov/blog/news/mayor-discusses-impact-of-ransomware-attack-on-new-bedfords-computer-system/.

[40] NEWS-DISPATCH, "Malware attack on county computers," 9 7 2019. [Online]. Available: https://www.thenewsdispatch.com/news/article_d9809e48-7e8d-52d5-9d08-5d6c1adab2a2.html.

[41] Inside Higher, "Hackers Demand $2 Million From Monroe," 15 7 2019. [Online]. Available: https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack.

[42] Associated Press, "Indiana county targeted in malware assault on computers," 24 7 2019. [Online]. Available: https://apnews.com/65b22b56e7384c7db4031a07c92c64f9.

[43] Fox 5 News, "Multiple Georgia state law enforcement agencies hit by ransomware attack," 28 7 2019. [Online]. Available: https://www.fox5atlanta.com/news/multiple-georgia-state-law-enforcement-agencies-hit-by-ransomware-attack.

[44] WTVY, "Houston County Schools pushes school start back further," 30 7 2019. [Online]. Available: https://www.wtvy.com/content/news/Houston-County-Schools-Announces-Additional-Delay-513399671.html.

[45] DIR, "Update on Texas Local Government Ransomware Attack," 5 9 2019. [Online]. Available: https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213.

[46] ZDNet, "Ransomware hits hundreds of dentist offices in the US," 29 8 2019. [Online]. Available: https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.

[47] Republican-American, "Wolcott school computers remain shut down a week after malware attack," 9 9 2019. [Online]. Available: https://www.rep-am.com/local/news-local/2019/09/09/wolcott-school-computers-remain-shut-down-a-week-after-malware-attack/.

[48] Campbell Country Health, "SERVICE DISRUPTIONS AT CCH; NO ETA," 20 9 2019. [Online]. Available: https://www.cchwyo.org/News/Press_Center/Health_News/2019/Service_Disruptions_at_CCH_no_ETA.aspx.

[49] The United States Conference of Mayors, "2019 Adopted Resolutions," 9 7 2019. [Online]. Available: http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%20and%20Social%20Justice.

[50] The Cybersecurity and Infrastructure Security Agency, "Steps to Safeguard Against Ransomware Attacks," 30 7 2019. [Online]. Available: https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks.

[51] The Cybersecurity and Infrastructure Security Agency, "CISA Insights: Ransomware Outbreak," 21 8 2019. [Online]. Available: https://www.us-cert.gov/ncas/current-activity/2019/08/21/cisa-insights-ransomware-outbreak.

[52] IBM, "LOCAL GOVERNMENT RANSOMWARE STUDY," 5 9 2019. [Online]. Available: https://www.ibm.com/downloads/cas/MKPQVOL6.

[53] CYBEREASON, "TRIPLE THREAT: EMOTET DEPLOYS TRICKBOT TO STEAL DATA & SPREAD RYUK," 25 4 2019. [Online]. Available: https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware.

[54] ZDNet, "Florida city fires IT employee after paying ransom demand last week," 1 7 2019. [Online]. Available: https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/.

[55] BANK INFO SECURITY, "Emotet Botnet Shows Signs of Revival," 26 8 2019. [Online]. Available: https://www.bankinfosecurity.com/emotet-botnet-shows-signs-revival-a-12964.

[56] Bleeping Computer, "Emotet Botnet Is Back, Servers Active Across the World," 23 8 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/emotet-botnet-is-back-servers-active-across-the-world/.

[57] Cybersecurity and Infrastructure Security Agency, "Alert (TA18-201A)," 20 7 2019. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-201A.

[58] SOPHOS, "Emotet:Nastier Than WannaCry and Harder to Stop," 7 2 2019. [Online]. Available: https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/emotet-nastier-than-wannacry-harder-to-stop-pdf-2-w-5139.pdf.

November 29, 2019

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
nttdata-cert@kits.nttdata.co.jp