Quarterly Report on Global Security Trends

4th Quarter of 2018

Table of Contents

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.

Attacks such as Web skimming by an attacking group "Magecart" and those using software supply chains have existed since before, which have been low in number and frequency, however are now increasing expanding their presence. With regard to data breach, an incident occurred in which a file "Collection #1" was disclosed, which contained aggregated account data leaked before.

Web skimming by an attacking group Magecart

"Web skimming" attacks have attracted many attentions, which compromise payment data in vulnerable online stores. Particular attention was paid to the method with which an attack grouping "Magecart" injected malicious code not only directly but also indirectly into online stores by compromising JavaScript libraries. With this attack, a wide range of stores was indirectly compromised. In addition to conventional security measures for vulnerability, it is important for online store suppliers to find signs of possible falsification.

Software supply chain attacks

Software supply chain attacks occurred several times in the past, and in this quarter, ASUS incident has attracted tremendous interest. This attack called "Operation ShadowHammer" delivered malware through the software supply chain for the utility software preinstalled in PCs manufactured by ASUS. Consequently, many ASUS PCs were infected. In addition, with signature to the qualified certificate, most security products could not detect this attack.

Distribution of data of over 100 million accounts

In data breach incidents, it has attracted tremendous interest that seven file groups containing a huge amount of account data as represented by Collection #1 were disclosed sequentially. These are huge file groups containing data of a total of 3.5 billion accounts, which are a collection of account data leaked over the internet in the past. The incident like this where account data list is exposed is a rare case, and basically attackers exchange data secretly over the dark web. We have to be aware that theft and leak of account data, and distribution of lists with collected account data occur regularly. Users need to verify that their account data is not leaked and take preventive measures such as the use of two-factor authentication or avoiding reuse of passwords.

Forecast

After the first quarter of 2019, the increase in the number of Web skimming attacks, list-based attacks exploiting a huge amount of leaked account data, and attacks on cryptocurrencies according to the increase in the market price is expected.

Web skimming attacks continue to be active, resulting in the increased number of online stores compromised. In addition, we can easily imagine that targeted and list-based attacks exploiting account data leaked in the fourth quarter of 2018 can occur. The number of attacks on cryptocurrencies decreased upon decrease in the market price of cryptocurrencies may increase according to the increase in the price.

2. Featured Topics

2.1. Web skimming

Web skimming is an attack to steal payment information entered online by injecting malicious code online instead of stealing payment data by altering ATMs or credit payment devices. In 2018, an attacking group using this attack presented topics. The group was named "Magecart" after "Magento", a platform for constructing major EC sites used worldwide, on which the group made attacks [1]. This group has existed since before and the incidents related to this group were covered twice in Report on Global Security Trends in the past [2] [3]. In the fourth quarter of 2018, activities by Magecart and Web skimming-related incidents were seen frequently, which were listed in Table 1.

Table 1：List of Web skimming-related events

No.	Date	Overview
1	Jan 7	A kitchen goods company, OXO International announced that its online store have been compromised for more than two years, resulting in possible leak of payment data [4]. A news medium BleepingComputer reported based on its original survey that skimming code has been injected into the company's online store [5].
2	Jan 16	Trend Micro discovered a new attack method for performing Web skimming by injecting malicious code indirectly into online stores by compromising the library for advertisement distribution [6]. Malicious code has been injected into legitimate JavaScript libraries provided by a French online advertisement company Adverline and Web skimming has been performed on 277 online websites.
3	Jan 17	A Dutch security researcher, Willem de Groot unveiled the vulnerability exploited by Magecart [7] [8]. It is a MySQL vulnerability that sends any local file on the client side when the client application connects to a malicious MySQL server. The attacker connected management MySQL client to the malicious MySQL server that he/she installed and read the file containing the administrator's password for the managed sites stored in the client.
4	Feb 22	A sports trading cards company, Topps announced that its customers' payment data has been leaked through Web skimming by Magecart [9]. The leaked data includes those of the customers who purchased products on Topps' online store between November 19, 2018 and January 9, 2019,
5	Mar 14	A news medium Security Affairs reported that a new Web skimming tool, JS Sniffer "GMO" was found in the survey by a security company, Group-IB [10]. It revealed that Web skimming using the tool has been performed on seven online stores including the website of FILA UK, a sports goods company.

No.	Date	Overview
6	Mar 20	A security company, RiskIQ announced that the online stores of bedclothes suppliers, MyPillow and Amerisleep suffered Web skimming attacks from Magecart [11]. MyPillow has been victimized by Web skimming between October and November, 2018. Web skimming attacks on Amerisleep started in December 2018 and skimming code was still active when the announcement was made.

The following explains conventional Web skimming methods used by Magecart, which are described in the report released by a security company, RiskIQ [12].

1. Guess ID/PW by a brute force attack on the management page and grasp the vulnerability that can be exploited by using the vulnerability scan
2. With the use of information in 1., attempt unauthorized login and alter the website contents to inject malicious code for Web skimming into the payment page
3. Send the user's payment data to the attacker's server upon entry of the data by the user on the online store

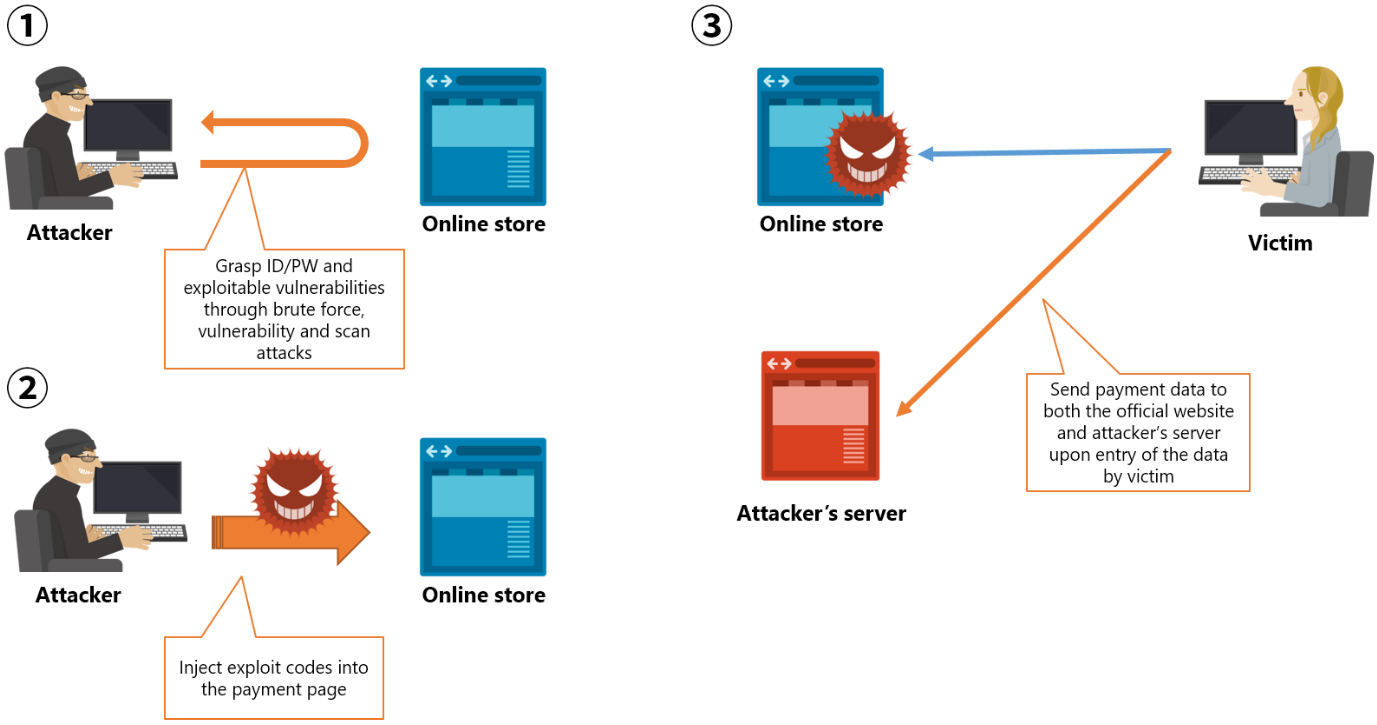

①
Attacker
Online store
Grasp ID/PW and exploitable vulnerabilities through brute force, vulnerability and scan attacks
②
Attacker
Online store
Inject exploit codes into the payment page
③
Online store
Victim
Attacker's server
Send payment data to both the official website and attacker's server upon entry of the data by victim

Figure 1: Flow of existing Web skimming
(Prepared by NTTDATA-CERT using data provided by RiskIQ [12])

The attack detected by Trend Micro in the fourth quarter of 2018 (Event No.2) used a method to inject malicious code for Web skimming indirectly into a lot of online stores by distributing JavaScript libraries compromised, exploiting the software supply chain, not a traditional method to inject malicious code for Web skimming by directly compromising online stores [6]. The following explains the method by using Figure 2 below:

1. Attacker compromises the environment of the supplier of advertising services
2. Attacker alters JavaScript libraries used for advertising distribution and injects malicious code for Web skimming. The compromised JavaScript libraries are delivered to online stores (e-commerce websites). Malicious code is loaded into online stores (e-commerce websites) that are using the libraries
3. Payment data is skimmed from online stores using malicious code upon payment by user
4. Skimmed payment data is sent to attacker's server.

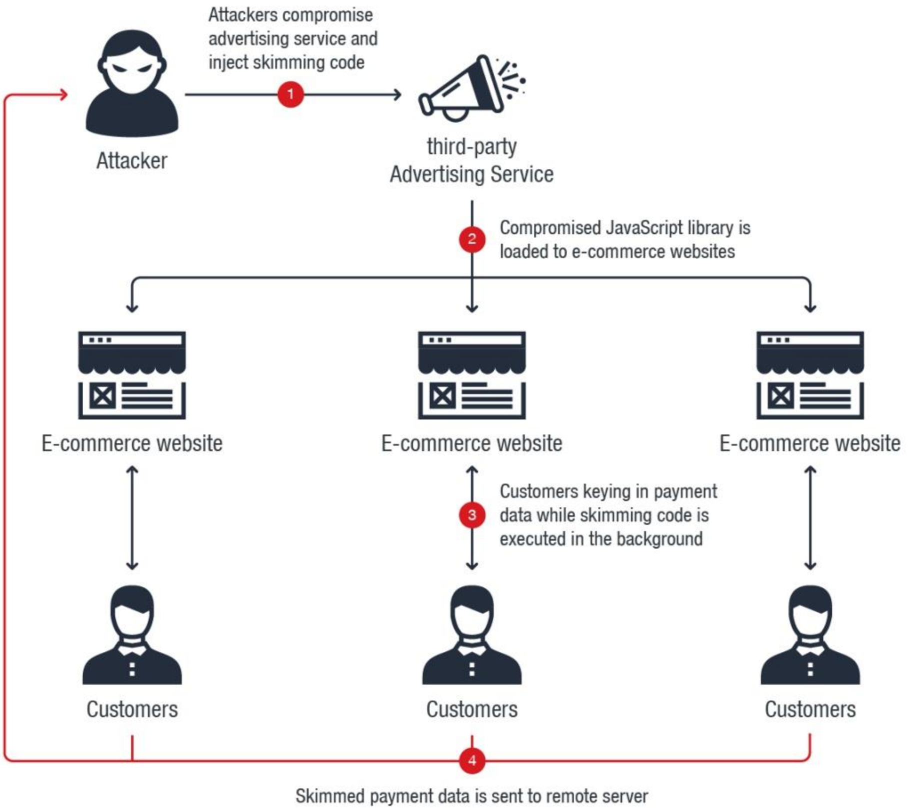

Attackers compromise advertising service and inject skimming code
1
Attacker
third-party Advertising Service
2
Compromised JavaScript library is loaded to e-commerce websites
E-commerce website
E-commerce website
E-commerce website
3
Customers keying in payment data while skimming code is executed in the background
Customers
Customers
Customers
4
Skimmed payment data is sent to remote server

Figure 2: Flow of new Web skimming (Reprinted from Trend Micro's security blog [6])

A major advantage of this means of indirectly injecting malicious code for Web skimming is stealing a large amount of data by installing the Web skimming mechanism in a wide range of online stores by just one compromise. Figure 3 shows the trend of the number of accesses to unauthorized domains through Web skimming activities detected by Trend Micro from the end of 2018 to the first week of January [13]. Installing the Web skimming mechanism exploiting the software supply chain increased the number of accesses detected from 1st to 2nd January, 2019.

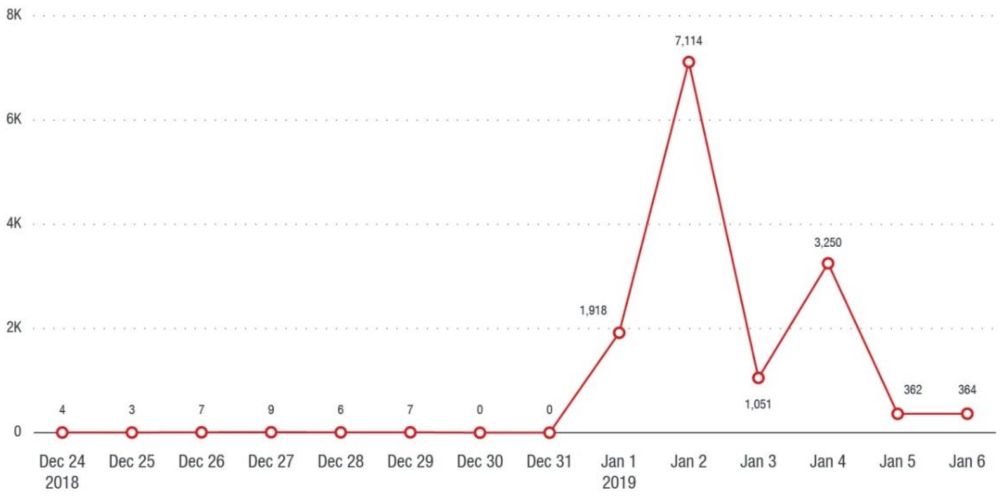


Figure 3: Number of accesses to unauthorized domains through Web skimming activities (Reprinted from Trend Micro's security blog [6])

This incident was only one case occurred in the fourth quarter of 2018 using the means of indirectly injecting malicious code for Web skimming because the means needs to hack the environment of the providers of robust JavaScript libraries or advertising services. Due to attacks becoming active, however, it is expected that Web skimming mechanism is installed in many online stores and payment data is stolen by using this indirect means together with the traditional means of injecting malicious code for Web skimming by directly compromising online stores. In order to prevent damage from Web skimming, it is recommended for online store providers to eliminate the vulnerability by timely updating the middleware and platform and to review the authentication system and security settings for more robust online stores. It is also recommended to only use reliable libraries and plugins for preventing damage from the indirect means, and not an effective measure, to consider the use of any solutions such as security diagnosis and Website Falsification Detection System for detecting compromised libraries as early as possible.

2.2. Supply chain attacks

Supply chain attack is now the term for two types of attacking methods [14].

The first attacking method is used as a foothold for attacks on less-secure organizations in distribution channels (supply chains) including business partners to make attacks on target organizations such as major companies and governmental organizations. This attack is newly ranked the fourth in the category of threats against organizations in the "10 Major Security Threats 2019" announced by IPA [15].

The second one is used as a foothold for attacks by distributing software with malware or exploit code injected through the software supply chain of the software development/distribution source. A supply chain attack with malware injected was made on "Transmission", the updater of P2P file sharing software for Mac in 2016 while in 2017, on "CCleaner", the installer of system cleaner software for Windows [16] [17]. In the fourth quarter of 2018, four events related to the second attack, so-called software supply chain attack occurred as shown in Table 2.

Table 2: List of events related software supply chain attack

No.	Date	Category	Overview
1	Jan 19	PHP PEAR	There was an evidence of an attack on the official website of the PEAR package management tool for PHP, and it was revealed that an altered installer (go-pear.phar) has been placed there [18].
2	Jan 22	Debian APT	A vulnerability was found in the APT package management tool for Debian-based Linux distribution. Exploiting this vulnerability could install malicious applications and execute any exploit codes [19].
3	Mar 13	Android SDK	Check Point discovered an adware campaign "SimBad" on the Google Play Store. An adware had been installed in an advertising SDK called RXDrioder and the adware was embedded in more than 200 applications developed using the SDK, resulting in 150 million downloads of the applications [20].
4	Mar 25	ASUS Live Update	Kaspersky Lab announced part of the results of a survey on the attack "Operation ShadowHammer", which distributes malware exploiting software "ASUS Live Update" provided by ASUS [21].

Out of these four events, the event related to ASUS attracted public attention. The attack named "Operation ShadowHammer" by Kaspersky Lab exploited "ASUS Live Update", an automatic update utility for PC manufactured by ASUS to distribute malware [22]. This utility software is preinstalled in most of the latest PCs manufactured by ASUS. The attacker injected a code to add malware functions to this utility software and added a code signature to the software using an official certificate stolen from ASUS. Then the attacker intruded into the official update server to deliver the compromised utility. Anti-virus software uses a code signature to verify if software is compromised. Therefore, anti-virus software could not detect this compromised utility software with a code signature added to the official certificate, resulting in more than 57,000 computers affected by the compromised software [23].

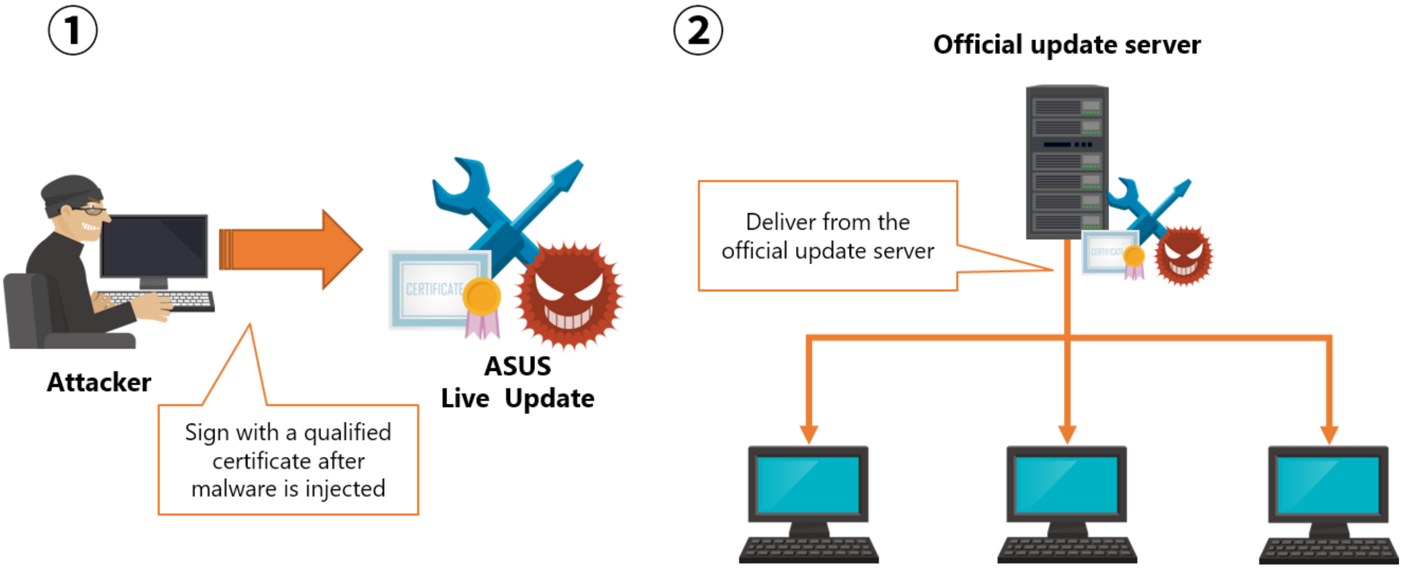

①
Attacker
Sign with a qualified certificate after malware is injected
CERTIFICATE
ASUS Live Update
②
Official update server
Deliver from the official update server

Figure 4：Flow of the Operation ShadowHammer attack
(Prepared by NTTDATA-CERT based on the Kaspersky Lab's information [22])

It is difficult for users to detect and overcome software supply chain attacks like this in their early stage. Manufacturers are recommended to not only preferentially reinforce the servers such as the update server, which can have a far reaching impact on users but also carefully manage important files including certificates to prevent them from being exploited by attackers.

2.3. Two-factor authentication

Two-factor authentication is a mechanism to verify the identity of a user by combining two factors out of the following: "what only the user knows", "what only the user owns" and "characteristics of the user (including fingerprints" [24]. As examples, the following combinations are available: a combination consisting of a combination of ID and password that only the user knows and one-time password contained in an SMS message received by the mobile phone that only the user owns; or one-time password created by an application on the smartphone device that only the user owns.

These combinations are safer than the conventional combination of ID and password because even if the combination of ID and password is compromised by means of a brute force attack or due to data breach, the attacker cannot login immediately. As shown in Table 3, however, an event occurred in the fourth quarter of 2018, which could threaten the safety of two-factor authentication.

Table 3: List of events related to two-factor authentication

No.	Date	Overview
1	Jan 2	A Polish security researcher, Piotr Duszyński released a tool "Modlishka" that can break two-factor authentication [25]. The tool works as a reverse proxy between a phishing website and a legitimate website to steal the data entered by the user and authentication data.
2	Feb 1	A news medium, Motherboard announced that two-factor authentication for the online service of MetroBank, a bank in England was broken, leading to bank deposits stolen [26]. The bank has used SMS message for delivering a one-time password for the second factor in two-factor authentication for remittance confirmation. The attacker intercepted SMS messages exploiting the vulnerability of the Signaling System No.7 used in the public telephone switching network to obtain a one-time password.

A tool "Modlishka" released by a Polish security researcher, Piotr Duszyński shown in Event No.1 above is a reverse proxy that works between a web browser and a legitimate website [27]. Authentication data entered in Modlishka by a user is sent to a legitimate website in real time, and a response from the legitimate website is displayed to the user via Modlishka (See Figure 5). Seen from the user, Modlishka displays the same processing results as when he/she enters his/her account information and other data in the legitimate website. Actually, however, the data entered by the user is just transferred to the legitimate website via Modlishka, and consequently all the data entered by the user falls into the attacker's hands.

In the demonstration video released [28], we can see the attacker who created a phishing website of Google and broke two-factor authentication using a Google's SMS message, which resulted in successful login.

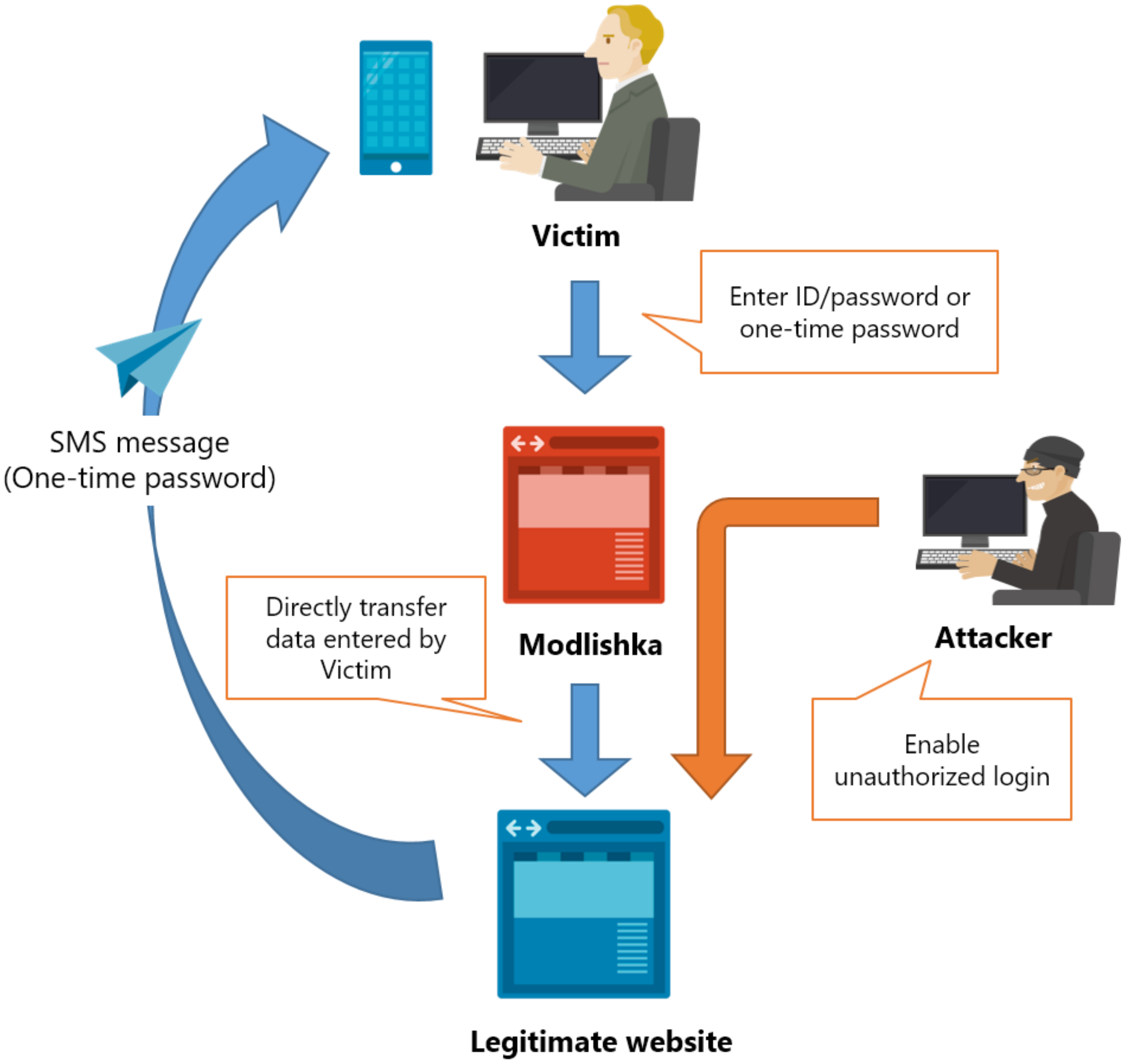

Victim
Enter ID/password or one-time password
SMS message (One-time password)
Modlishka
Directly transfer data entered by Victim
Attacker
Enable unauthorized login
Legitimate website

Figure 5: Flow of Modlishka communication
(Prepared by NTTDATA-CERT based on Piotr Duszyński'a blog [25])

In Event No.2 related to MetroBank in England, the attacker broke two-factor authentication by exploiting the vulnerability of SS7(Common Channel Signaling System No.7), a signal protocol for the public telephone switching network and intercepting an SMS message to the affected user. SS7 is an international standard used throughout the world including Japan. However, SS7 is subject to use only between telecommunications carriers without no authentication process for command senders, resulting in all commands processed, which allows the attacker to receive SMS messages by impersonating the receiver. In 2015, a report said that communication could be interrupted by using this vulnerability [29]. In 2017, an incident was reported in which an SMS message was interrupted and two-factor authentication was broken in a bank in Germany like this event, leading to illegal money transfer [30].

These two events revealed that the use of two-factor authentication does not necessarily ensure the security depending on how it is implemented. Piotr Duszyński says in his blog that the use of hardware tokens with FIDO U2F protocols as the second authentication factor can make two-factor authentication safer. In FIDO authentication, a key is created on a service basis, and tokens and clients supporting FIDO establish communication for services and authentication on behalf of users. This can prevent a second factor from being leaked to SMS as well as users from entering a second factor in unauthorized websites, which can prevent events like the above.

Service providers need to provide more secure authentication like FIDO while users need to select more secured authentication, which can reduce the number of security incidents.

3. Data Breach

On January 19, 2019, an Australian security researcher Troy Hunt published analysis results of a file group “Collection #1” [31]. “Collection #1” had contained the data of 773 million accounts, which raised public attention. In addition, the report by a security journalist Brian Krebs revealed that “Collection #1” is a part of a larger file group “Collection”. Data of a total of over 3.5 billion accounts had been included in them [32].

Brian Krebs said that he contacted a user called “Sanixer” who disclosed “Collection #1” by using an instant message system “Telegram” and made a survey. Sanixer told Brian Krebs that “Collection #1” was the data of two or three years ago, he (she) had additional account data other than a larger file group “Collection” and had a total of more than four terabytes of new account data collected within a year.

Recorded Future also made a survey of attackers related to “Collection #1” [33]. Recorded Future said in a report that a person called “C0rpz” online collected data of billions of accounts in the past three years. The report also said that “C0rpz” sold the account data to “Sanixer” who Brian Krebs of KrebsOnSecurity contacted and a person called “Clorox”.

The following shows the history of selling/purchasing account data relating to “Collection #1” and disclosure of related information;

Table 4: History of selling/purchasing account data relating to “Collection #1” and disclosure of related information

Date	Overview
April 2018	″ANTIPUBLIC #1″ was shared over the internet
October 2018	Collection #1-related data was posted to an underground forum for the first time
Around the end of 2018	″Collection #1″ appeared on a dark web forum
Around January 7, 2019	The presence of ″Collection #1″ was revealed on a hacker forum
Around January 6 to 12, 2019	Troy Hunt received multiple reports on “Collection #1”
January 17, 2019	Troy Hunt released the analysis results
	Brian Kreb released a report on a total of seven packages including “Collection #1”

Table 5: Information on "Collection"

Name	Size
ANTIPUBLIC #1	102.04 GB
AP MYR & ZABUGOR #2	19.49 GB
Collection #1	87.18 GB
Collection #2	528.50 GB
Collection #3	37.18 GB
Collection #4	178.58 GB
Collection #5	40.56 GB

Soliton Systems analyzed "Collection #1" and extracted email addresses and file names with ".jp" at the end to calculate the number of accounts related to Japanese people or organizations [34]. There were a total of 20.02 million accounts with a combination of an email address and password having a Japanese-like name, and out of these, 8.03 million accounts seemed relatively new. There were 402 Japanese Web service sites from which account data is leaked while 6 service websites were suspected to leak relatively new account data.

We have to be aware that theft and leakage of account data, and distribution of lists with collected account data always occur. These lists are usually exchanged on a dark website; therefore these are less likely to be disclosed over the internet like "Collection #1". Easy acquisition of account data that is normally exchanged on a dark web secretly allows poorly skilled attackers to easily carry out list-based attacks. Since there are account data undisclosed, we need to consider both cases for taking measures. As measures against list-based attacks exploiting account data, the use of two-factor authentication is strongly recommended. Using two-factor authentication can prevent unauthorized login even if account data is leaked. In order to eliminate the risk of unauthorized login to a service using account data leaked from another service, prohibiting password reuse is crucial.

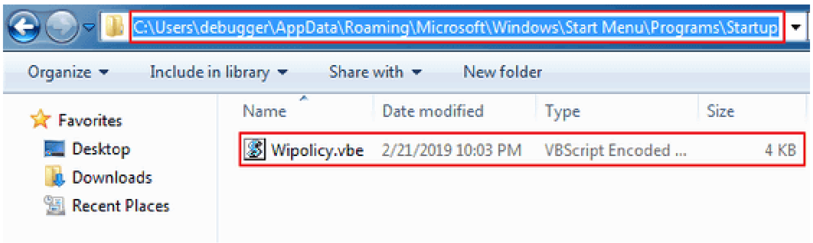
Besides "Collection #1"-related data breach, multiple large-scale data breach incidents occurred or detected in the fourth quarter of 2018. Some data breach incidents occurred or identified are listed as below. Compared to the third quarter of 2018 or before, this quarter is characterized by multiple incidents involving leakage and disclosure of a large amount of data of over 100 million accounts.

Table 6: Data breach incidents

Date	Overview	Amount of affected data
Dec 28	Bob Diachenko of HackenProof discovered that resume data of over 200 million Chinese job applicants are accessible on MongoDB without authentication [35]. The disclosed date is unknown, and the database was protected one week after discovery of disclosure.	200 million
Jan 21	It was revealed that an online casino group leaked more than 108 million pieces of data. Those include information about customer's personal data and deposit and withdrawal data. There is a concern that rich customers can be targeted for fraud or theft [36].	108 million
Jan 25	OGIS Research Institute announced that data of 4.8 million customers of "Taku-File Bin", a high volume file transfer service was leaked due to unauthorized access to some servers, which corresponds to the number of all registered users. According to a survey, unauthorized access probably came from overseas [37].	4.8 million
Feb 11	An attacker called "Gnosticplayers" sold personal information four times between February and March on a dark web "Dream Market". The number of pieces of information sold is 620 million in the first selling activity, 127 million in the second, 93 million in the third and 26.5 million in the fourth [38].	866.5 million (Total amount for four times)
Feb 25	Security researchers Bob Diachenko and Vinny Troja discovered non-password-protected MongoDB. The database was owned by Verifcations.io, an email marketing company, which had contained approximately 809 million personal data records. Bob Diachenko said that personal data that might be leaked from this DB is not the same as those identified in "Collection #1" [39].	809 million
Mar 8	On Mar 8, Citrix announced that its internal network suffered unauthorized access. The unauthorized access was detected by information provided by Resecurity and FBI. Data of more than six terabytes was stolen by means of a method called password spraying [40].	6 terabytes (Number of pieces of information unknown)

4. Vulnerability

On February 20, 2019, Check Point Software Technologies disclosed the vulnerability of directory traversal of "WinRAR", a file compression/decompression utility for Windows (CVE-2018-20250) [41]. This vulnerability may affect all versions released in the past 19 years. The vulnerability is located in the "UnAceV2.dll" library that decompresses archives in ".ace" format. Check Point is warning about the possibility that attackers install malware in the Windows startup folder exploiting this vulnerability.



C:\Users\debugger\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Name	Date modified	Type	Size
Wipolicy.vbe	2/21/2019 10:03 PM	VBScript Encoded ...	4 KB

Figure 6：Example of a file located in the startup folder separated from image or text files (Reprinted from 360 Threat Intelligence Center's blog [42])

This vulnerability was detected in 2018, and then on January 28, 2019, "WinRAR 5.70 Beta 1" was released for addressing it. WinRAR developers terminated support for the ".ace" format to avoid the vulnerability. Since the vulnerability was disclosed, however, there has been many cases found where the vulnerability is exploited. The located file contains a wide variety of documents from technical documents and adult graphics via non-discriminatory attacks, to documents related to the Ukrainian laws, and United Nations (UN) and human rights via targeted attacks. Attackers can create any files in any locations by exploiting the vulnerability, which may cause possible risk of virus infection. WinRAR users need to take appropriate measures including update and take care in handing files whose source is unknown.

Table 7 describes the vulnerabilities disclosed in the fourth quarter of 2018, focusing mainly on zero-day vulnerabilities, exploited vulnerabilities and highlighted vulnerabilities.

Table 7: Other vulnerabilities including zero-day and highlighted vulnerabilities

Disclosed date	Product	Vulnerability number	Overview
Jan 9	IDenticard PremiSys Access control system	CVE-2019-3906 CVE-2019-3907 CVE-2019-3908 CVE-2019-3909	Tenable Research detected four vulnerabilities in PremiSys systems of IDenticard and disclosed them on Jan 14 [43]. Exploiting this vulnerability can implement various actions with administrator privileges. IDenticard has more than tens of thousands of customers including global companies, educational institutions, medical facilities and governmental organizations. A patch program was provided by IDenticard on Jan 31.
Jan 16	ES File Explorer File Manager (Android)	CVE-2019-6447	A vulnerability to input validation is detected in "ES File Explorer File Manager", an application for Android that has achieved over 500 million downloads since 2014. The HTTP server runs upon opening the application, which enables arbitrary code execution from the same network. The port remains opened even if the application is deleted [44].
Jan 25	Cisco RV320, RV325 Dual Gigabit WAN VPN routers	CVE-2019-1652 CVE-2019-1653	Data breach and command injection vulnerabilities were detected in Cisco RV320 and RV325 Dual Gigabit WAN VPN routers. On Jan 25, they were fixed by Cisco by applying an update, Bad Packets Report reported, however, that these vulnerabilities have been targeted for cyber attacks and prompted users to check the exploit code disclosed and apply a patch on Jan 26 [45].
Jan 25	Ttal Donations (WordPress)	CVE-2019-6703	A vulnerability was found in "Ttal Donations", a plugin for WordPress provided by Calmar Webmedia, which may allow the administrator rights of the website to be hacked. Exploiting this vulnerability enables to create a new user and grant it the administrator rights, which allows it to access the data that it normally cannot access. According to Defiant, maintenance has likely not been provided [46].
Feb 7 * First report on relevant information was made on Jan 29	iOS, macOS	CVE-2019-6223 CVE-2019-7286 CVE-2019-7287	A vulnerability of FaceTime video call function attracted public attention, which allows users to hear the voice of a callee without any operation by the callee. The version with this vulnerability modified also included modifications for two zero-day vulnerabilities that could enable privilege escalation and arbitrary code execution [47]. Additionally Google's Project Zero disclosed a serious zero-day vulnerability to macOS kernel and PoC code [48].

Disclosed date	Product	Vulnerability number	Overview
Feb 11	runc	CVE-2019-5736	A vulnerability was detected in "runc", a container runtime used by Docker and Kubernetes. Exploiting this vulnerability allows a malicious container to overwrite the runc binary and execute arbitrary code on the host with root privileges. This could affect the whole container, causing damage to hundreds to thousands of containers, which raised much attention [49].
Feb 20	Drupal	CVE-2019-6340	A vulnerability was detected in Drupal, which enables remote arbitrary code execution without authentication. This vulnerability is affected when the module using REST API is enabled. The exploit code was released immediately. According to LAC, many attempts to check the version of Drupal were observed on the next day after the vulnerability was disclosed [50].
Mar 1	Adobe ColdFusion	CVE-2019-7816	A vulnerability was found in Adobe ColdFusion, which allows attackers to upload a file to a directory viewable on the Web by avoiding restrictions on file upload. Attackers may execute arbitrary code with ColdFusion's executing user privileges. Adobe had already been informed of exploits of this vulnerability at the time of disclosure of this vulnerability [51].
Mar 1	Google Chrome	CVE-2019-5786	Google announced a UAF (Use After Free) vulnerability in Chrome's FileReader API on Mar 1 [52]. According to the Google security team, it has already been attacked by exploiting this vulnerability before the patch is released on 3/1. This is exploited together with a local privilege-escalation vulnerability that occurs in the Windows win32k.sys kernel driver, which enables remote arbitrary code execution [53].
Mar 13 *First report on relevant information was made on Mar 1	Windows	CVE-2019-0797 CVE-2019-0808	Out of vulnerabilities fixed with Microsoft's monthly patch update, two are a zero-day vulnerability in "Win32k". Exploiting these vulnerabilities may enable remote code execution. The "CVE-2019-0808" vulnerability has already been pointed out by Google's researcher, which are combined with the Google Chrome vulnerability above for attacks [54] [55].

5. Malware/Ransomware

Table 8 and Table 10 show malware driving attack campaigns, ransomware and other malware identified in the fourth quarter of 2018.

Table 8: Malware campaigns identified/reported in the fourth quarter of 2018

Month	Name	Overview
Jan.	Emotet (Malware name)	Melon Security's researcher made a report on the "Emotet" campaign that is enhanced so as to affect more systems. It exploits macros in XML files disguised as Word documents. A wide variety of industries, especially healthcare industry had been targeted [56].
Jan.	SpeakUp (Malware name)	Check Point Software Technologies identified an attack campaign using a Trojan, dubbed "SpeakUp". It targets Linux hosted in a cloud environment such as AWS. Servers in China, India, Southeast Asia and South America had been targeted [57].
Jan.	Ursnif (Malware name)	Cisco Talos made a report on a new campaign that distributes the "Ursnif" infostealer malware. It infects "Ursnif" via Word documents containing malicious VBA macros. After infection, compressing data stolen using CAB files can prevent it from being detected [58].
Jan.	Love you	An email malspam campaign "Love You" was identified. The email title was "I Love You" or "My love letter for you" written in English, which had consisted of only emoticons before. It can give rise to mixed infections in ransomware, coin miner or spambot [59].
Feb.	Astaroth Trojan (Malware name)	A Trojan that exploits legitimate process or anti-virus software on Windows OS was detected in October, 2018. The target countries include Brazil and European countries. It was reported in February as an on-going campaign [60].
Feb.	Shlayer (Malware name)	A new type of malware "Shlayer" targeting macOS was found. It was distributed as an update to Adobe Flash. Affected legal domains were used in some cases, and most of DMG files used had been signed with a legitimate Apple Developer ID [61].
Feb.	Operation Pistacchitto	Operation Pistacchitto is a malware campaign that has been active since 2016, which is originated from Italy. The spread through the Github platform was reported in February. It infects via malicious links in spam emails. A variant of existing malware was also identified, which targets not only Windows but also Android, Linux and macOS [62].

Table 9: Ransomware identified/reported in January to March

Month	Name	Overview
Jan.	Anatova	Anatova is ransomware discovered by a McAfee's researcher, which is equipped with a strong encryption function and module type expansion [63]. It makes users click on the icons disguised as those of games or applications to download ransomware. It spreads via peer-to-peer networks.
Feb.	Jokeroo	"Jokeroo" is a new RaaS that has been promoted on the Twitter and distributed in an underground hacking forum "Exploit.in". Initially it had pretended to be related to GandCrab, its developer, however, unveiled that there is no relation. It demands money by encrypting files [64].
Mar.	CryptoMix	A variant of "CryptoMix" ransomware was discovered. It targets not individual computers but the whole network. The executable file is signed by code signing, which is not detected by anti-virus software. It disables anti-virus software upon start of the computer to close all files for encryption [65].
Mar.	JNEC.a	JNEC.a is ransomware that spreads exploiting the WinRAR vulnerability (CVE-2018-20250). It changes the extension to ".Jnec" by encrypting files. It has a feature of generating Gmail addresses for receiving decryption keys after payment is made [66].
Mar.	Yatron	"Yatron" ransomware tries to spread to other computers on the network, exploiting EternalBlue and DoublePulsar malware that are infecting PCs. It deletes files if payment is not made within 72 hours [67].
Mar.	LockerGoga	LockerGoga injects and executes ransomware in PCs by exploiting a system management tool "PsExec". Paying ransom demands prevents victims from having an opportunity to decrypt files; therefore it was spread for the purpose of suspending business. In January, an attack on Altran Technologies was reported. Some European companies were affected by it [68].

Table 10: Other malware identified/reported in January to March

Month	Name	Overview
Jan.	Vidar	According to a malware researcher, a new infostealer "Vidar" was spread by using Fallout Exploit Kit. Fallout Exploit Kit was used also to spread GandCrab ransomware. Vidar is used for the purpose of stealing process information [69].
Jan.	CookieMiner	"CookieMiner" steals cookies from web browsers such as Chrome and Safari that run on Apple Mac computers to steal user names, passwords, credit card data and SMS data stored in the browser [70].
Jan.	Rietspoof	Rietspoof propagates via instant messaging applications such as Facebook's Messenger and Skype. According to a report from a security company Avast, this was found in August 2018, and its propagation became stronger in January 2019. It stays on the affected host to try to download other malware [71].
Jan.	TrickBot (Variant)	A new module "pwgrab" was added to steal authentication data from remote desktop applications VNC, PuTTY and RDP. Emails with Excel files attached, which contain malicious macros were identified as a route of infection [72].
Jan.	Mirai (Variant)	A variant of "Mirai" was reported, which is known that it attacks IoT devices with vulnerable settings and weak passwords. It infects a wide variety of IoT devices including devices for digital signage and wireless presentation systems [73]. Other various variants of "Mirai" have been identified.
Feb.	Winpot	Winpot is malware used in jackpot attacks that steal money by compromising ATMs. It mimics the slot's play screen. It accesses ATMs physically or over the network and installed [74].

6. Trends by Category

6.1. Trends of government-/public sector-led security measures

In this fourth quarter of 2018, security measures and bills led by the government and public sectors were introduced mainly in U.S.

Table 11: List of events related to government-/public sector-led security measures

No.	Date	Country/region	Overview
1	Jan 16	U.S.	The U.S. DARPA[1] announced a project "GAPS" for the purpose of creating a solution that enables to track the information and communication between systems in a safe and identifiable state [75]. The final goal of this project is to develop hardware and software architecture that can physically check information transfer between different security levels and high-risk transactions.
2	Jan 16	U.S.	A nonpartisan group of Diet members introduced a bill calling for the establishment of "Office of Critical Technologies and Security" in the White House to both the U.S. Senate and House [76]. This has a purpose to fight state-sponsored technology theft.
3	Jan 30	U.S.	The Department of Justice announced that FBI and AFOSI[2] would take action to investigate and take down the botnet used by North Korean hackers [77]. According to the amended Rule 41 in the Federal Rules of Criminal Procedure, they can not only investigate and take down the bonnet but also contact affected terminal users for informing them of the damage through ISP upon receipt of a court order or search warrant.
4	Feb 15	U.S.	A news medium delmarva now. reported that a new bill was submitted to the Maryland General Assembly, which calls for a heavier penalty on ransomware attacks [78]. It imposes a fine of up to 100,000 USD (13 million yen) and 10 years' imprisonment on an act causing a loss of 1,000 USD (approx. 130,000 yen) or more, which is regarded as a serious crime.
5	Feb 20	Japan	National Institute of Information and Communications Technology (NICT) kicked off an effort "NOTICE" to scan IoT devices on the internet and notify ISPs of the information of devices that may be exploited [79].

[1] the Defense Advanced Research Projects Agency

[2] U.S. Air Force Office of Special Investigations

No.	Date	Country/region	Overview
6	Feb 20	Russia	A news medium BBC reported that Russia's parliament passed a bill to ban the use of smartphones by Russian military soldiers on duty [80]. The purpose of this bill is to ban connection to the internet, taking pictures and posting on SNS to address national security problems including confidential data breach.
7	Feb 24	India	A new medium E Hacking New reported that the Indian government was going to install a DNS server that has a function to protect users from malware and phishing attacks [81]. The server displays a pop-up message when a user access a suspicious website to alert him/her.
8	Mar 18	EU	The EU Council adopted an EU Law Enforcement Emergency Response Protocol to prepare for major cross-border cyber attacks [82]. Europol plays a key role.
9	Mar 25	U.S.	NIST[3] released a draft of SP 800-204 that describes security policies for microservice-oriented application systems [83].

[3] National Institute of Standards and Technology

6.2. GDPR-related events

After the enforcement of the EU General Data Protection Regulation (GDPR), the number of violations reported and the number of sanctions with a fine imposed by the data protection authorities of EU member states has increased. In the fourth quarter of 2018, besides sanctions with a fine, concrete behavioral instructions, ideas for technologies and mutual approach between EU and Japan became effective.

Table 12: List of GDPR-related events

No	Date	Country/region	Overview
1	Jan 3	Portugal	A new medium iapp reported that the Portuguese Data Protection Authority CNPD[4] imposed a 400,000 euro fine on the Barreiro Montijo Hospital for violations of the GDPR [84].
2	Jan 21	France	The French data protection authority CNIL[5] imposed a fine of 50 million euros on Google for violations of the GDPR [85]. This is according to the investigation performed on May 25, 2018 by noyb, an Austrian non-profit organization for privacy enforcement upon receipt of a compliant.
3	Jan 23	Japan	A framework for mutual and smooth transfer of personal data between Japan and EU came into force [86]. This framework has been established where the Personal Information Protection Commission provides EU with requirements based on Article 24 in the Personal Information Protection Law while the European Commission determines that Japan has an adequate level of data protection based on Article 45 in GDPR.
4	Jan 24	EU	Google announced that it would file a complaint about the fine for GDPR violations [87].
5	Jan 28	EU	The European Commission disclosed that the total number of GDPR violations reported by the data protection authority of each country reached more than 95,000 in eight months after the GDPR becomes effective [88].
6	Mar 7	Netherlands	DPA[6] represented its view that a function to ask website visitors for consent to be tracked for advertising purpose, so-called a cookie wall is not appropriate for the GDPR [89]. This is in response to complaints from users who were refused access to the website because of refusal to consent.
7	Mar 26	Poland	The Office for Personal Data Protection in Poland (UODO[7]) imposed a fine of 220,000 euros on a digital marketing company Bisnode that has a branch office in Poland for violations of the GDPR while called for contacting approximately 5.7 million people who had received no notification required in Article 14 within three months [90].

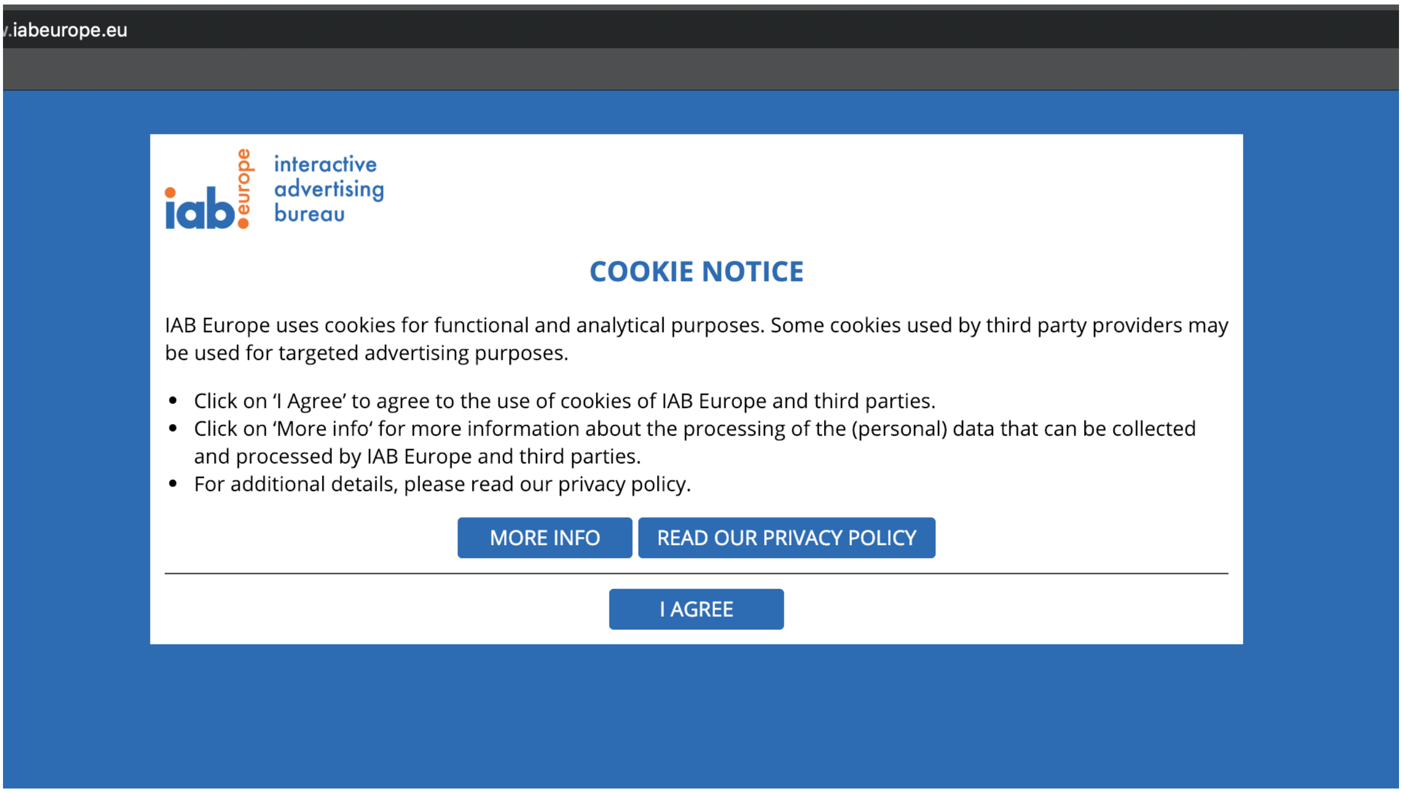
[4] Comissão Nacional de Protecção de Dados

[5] Commission Nationale de l'Informatique et des Libertés

[6] The Dutch Data Protection Authority

[7] Urzędu Ochrony Danych Osobowych

With regard to Event No.6 in the Netherlands, the Dutch Data Protection Authority (DPA) represented its view that cookie walls that frequently appear on recent websites (See Figure 7) do not meet the requirements for the GDPR. A cookie wall is a function to ask website visitors for consent to track their information when they access the website for advertising purpose. DPA received complaints from many users who were refused access to the website because of refusal to consent, and decided to release guidance on cookies. This guidance provides the Authority’s view and asks for visitors' consent to use different tracking software such as tracking cookies and tracking pixels.



COOKIE NOTICE

IAB Europe uses cookies for functional and analytical purposes. Some cookies used by third party providers may be used for targeted advertising purposes.

- Click on ‘I Agree’ to agree to the use of cookies of IAB Europe and third parties.
- Click on ‘More info’ for more information about the processing of the (personal) data that can be collected and processed by IAB Europe and third parties.
- For additional details, please read our privacy policy.

Figure 7: Example of a cookie wall (Reprinted from TechCrunch [91])

In Event No.7 in Poland, a digital marketing company Bisnode headquartered in Sweden, having a branch office in Poland was imposed a 220,000 euro fine for failure to fulfill its notification obligation stipulated in Article 14 in the GDPR. Article 14 of the GDPR requires that data administrator notifies users involved of the use of their personal information that was not directly obtained by data administer. In this case, Bisnode sent a notification via email to approximately 680,000 recipients whose email address was known after the report was made, for others, however, Bisnode provided information only on the website [92]. In response, UODO called for contacting the remaining 5.7 million recipients in some way.

7. Forecast on the 1st Quarter of 2019

Trends in the first quarter of 2019 (from April to June) are forecasted as follows: increase in damage due to Web skimming attacks; exploiting account data leaked; and increase in the number of attacks according to the increase in the market price of cryptocurrencies.

Increase in damage due to Web skimming attacks

Damage from Web skimming attacks has occurred continuously. An attacking group "Magecart" carries out Web skimming attacks on "Magento" that has been globally ranked as one of the top platforms used for EC site construction. The attacker may launch another Web skimming attacks through unauthorized access, targeting other platforms ranked high in use for EC site construction. Damage due to Web skimming attacks is expected to occur continuously in the future. In Japan, "Magento" has not been used so much; therefore domestic damage from Web skimming attacks was not frequent in the fourth quarter of 2018. Popular platforms for EC site construction used in Japan include "Color Me Shop", "MakeShop" and "eStore" that are Japan-specific. That may be why domestic Web skimming damage is lower than global damage. Some platforms for EC site construction that are highly used in Japan, however, use globally popular content management systems (CMS). If attackers find vulnerabilities of such CMS, domestic platforms for EC site construction can be attacked, resulting in damage caused by Web skimming. Online store suppliers and users need to be aware of not only failure in the EC site design and unauthorized login through brute force attacks but also Web skimming by exploiting vulnerabilities of the software constituting the platform and CMS' plugins containing malicious code.

Exploiting account data leaked

In the fourth quarter of 2018, a series of lists such as "Collection #1" containing a large amount of account data were disclosed over the internet. Easy acquisition of account data that is normally exchanged on a dark web secretly allows poorly skilled attackers to easily carry out list-based attacks. Consequently, attacks exploiting these disclosed data are expected to be frequent. This can lead to incidents of Web skimming attacks mentioned earlier. In order to prevent unauthorized login by exploiting these account data, it is strongly recommended to use two-factor authentication. Prohibiting reuse of the same password in another cloud service is crucial.

Increase in the number of attacks on cryptocurrencies

According to the analysis results of the collected data on cryptocurrency-related incidents, the number of attacks targeting cryptocurrencies was low, causing a small damage in the fourth quarter of 2018. As forecasted in the third-quarter report of 2018, this is because attackers changed the target of attacks from cryptocurrencies to others due to the decrease in the market price of cryptocurrencies. Currently, however, the market price of cryptocurrencies is on the rise again. Thus it is expected that cryptocurrency attacks will probably increase again in the first quarter of 2019. It is also expected in the first quarter of 2019 that attacks targeting service providers or users of cryptocurrency exchanges to directly steal cryptocurrencies will be more frequent than those targeting PC resources such as mining. Attacks targeting cryptocurrencies can vary according the market price of cryptocurrencies.

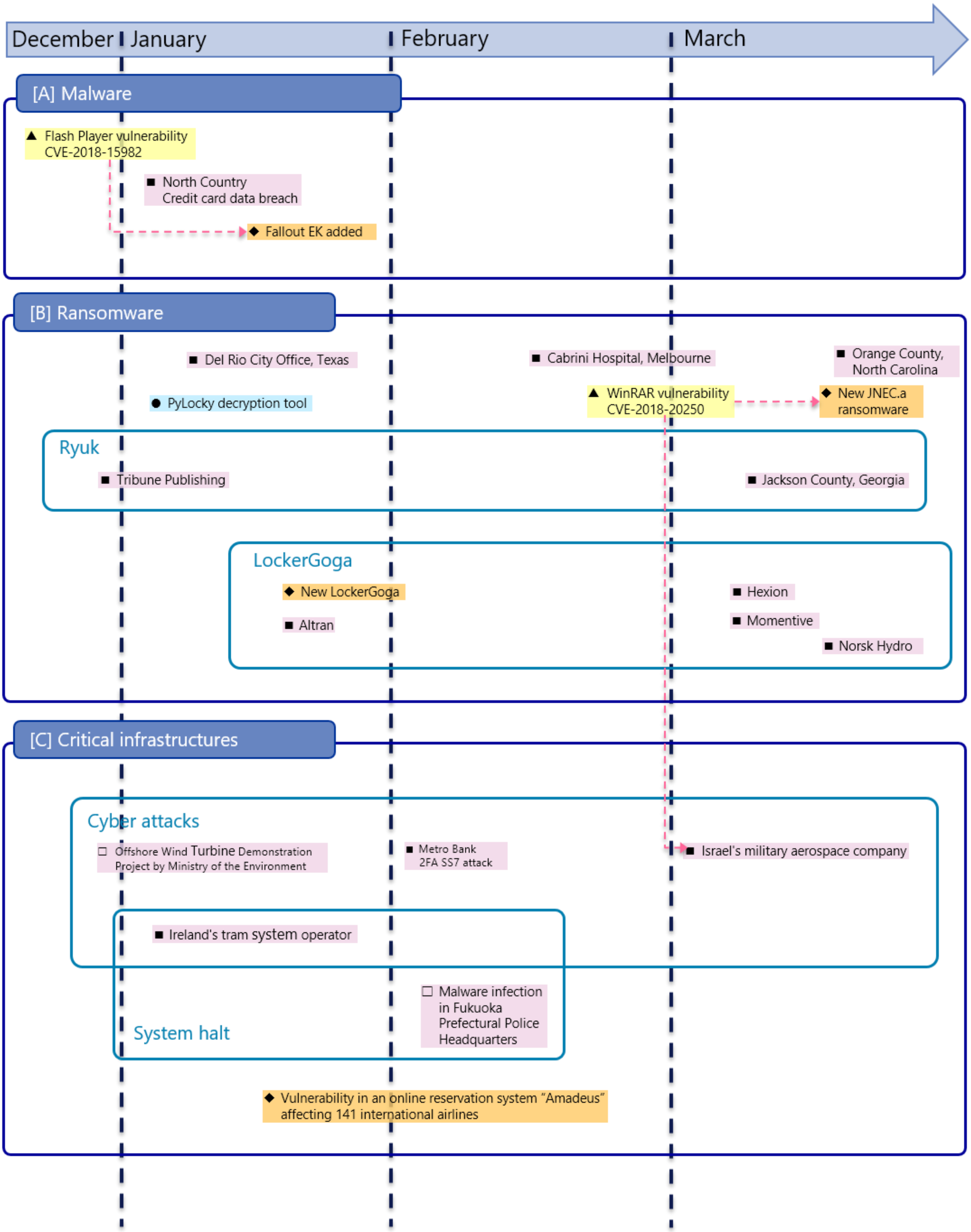
8. Timeline of 4th Quarter of 2018

*Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○:Domestic
▲■◆●:Global/Overseas

△▲:Vulnerability
□■:Incident

◇◆:Threat
○●:Measure



December | January | February | March

[A] Malware

▲ Flash Player vulnerability CVE-2018-15982

■ North Country Credit card data breach

◆ Fallout EK added

[B] Ransomware

■ Del Rio City Office, Texas

■ Cabrini Hospital, Melbourne

■ Orange County, North Carolina

● PyLocky decryption tool

▲ WinRAR vulnerability CVE-2018-20250

◆ New JNEC.a ransomware

Ryuk

■ Tribune Publishing

■ Jackson County, Georgia

LockerGoga

◆ New LockerGoga

■ Altran

■ Hexion

■ Momentive

■ Norsk Hydro

[C] Critical infrastructures

Cyber attacks

□ Offshore Wind Turbine Demonstration Project by Ministry of the Environment

■ Metro Bank 2FA SS7 attack

■ Israel's military aerospace company

■ Ireland's tram system operator

□ Malware infection in Fukuoka Prefectural Police Headquarters

System halt

◆ Vulnerability in an online reservation system "Amadeus" affecting 141 international airlines

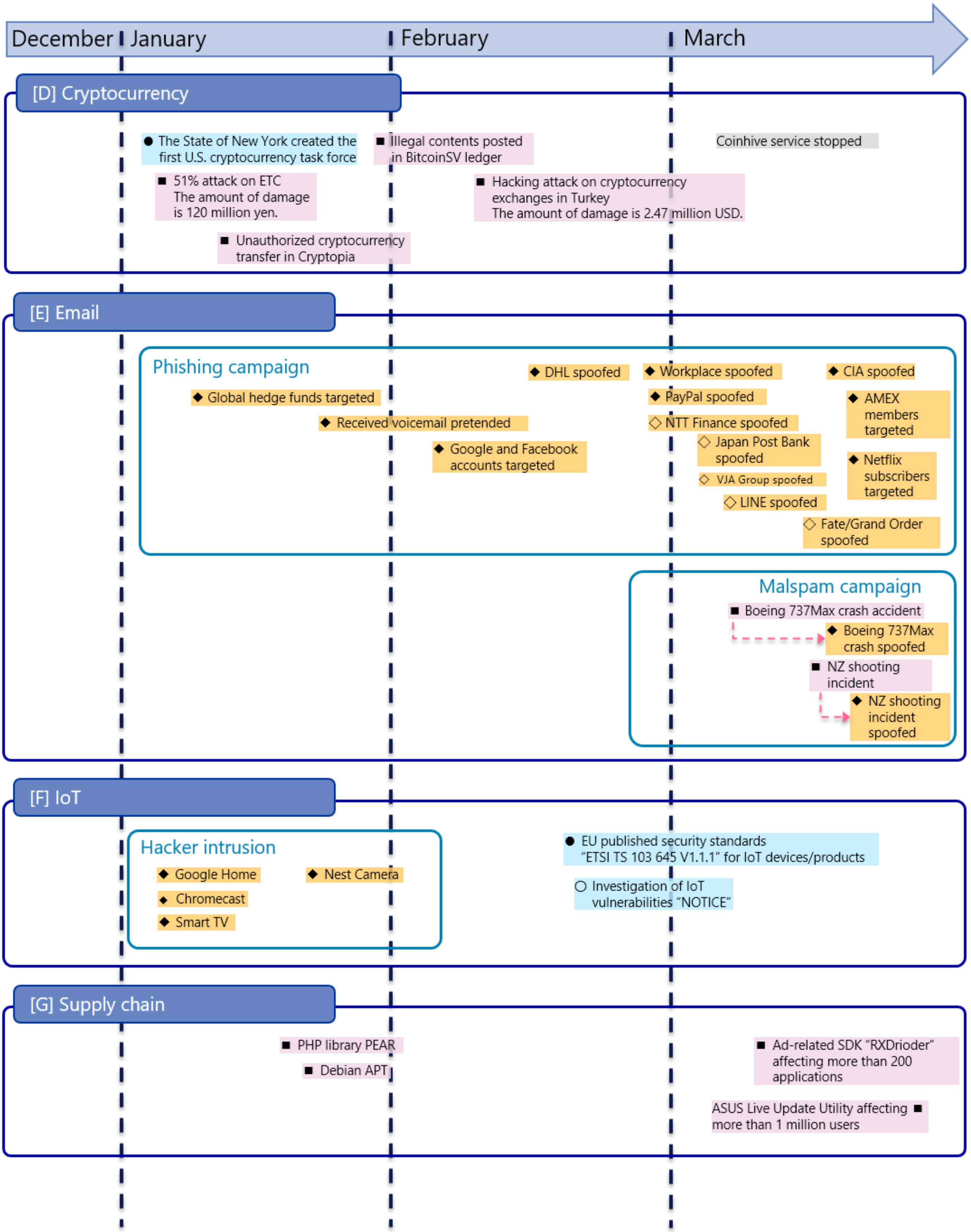
Timeline of 4th Quarter of 2018

*Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○:Domestic
▲■◆●:Global/Overseas

△▲:Vulnerability
□■:Incident

◇◆:Threat
○●:Measure



December | January | February | March

[D] Cryptocurrency

- ● The State of New York created the first U.S. cryptocurrency task force
- ■ 51% attack on ETC The amount of damage is 120 million yen.
- ■ Unauthorized cryptocurrency transfer in Cryptopia
- ■ Illegal contents posted in BitcoinSV ledger
- ■ Hacking attack on cryptocurrency exchanges in Turkey The amount of damage is 2.47 million USD.
- Coinhive service stopped

[E] Email

Phishing campaign

- ◆ Global hedge funds targeted
- ◆ Received voicemail pretended
- ◆ Google and Facebook accounts targeted
- ◆ DHL spoofed
- ◆ Workplace spoofed
- ◆ PayPal spoofed
- ◇ NTT Finance spoofed
- ◇ Japan Post Bank spoofed
- ◇ VJA Group spoofed
- ◇ LINE spoofed
- ◆ CIA spoofed
- ◆ AMEX members targeted
- ◆ Netflix subscribers targeted
- ◇ Fate/Grand Order spoofed

Malspam campaign

- ■ Boeing 737Max crash accident
- ◆ Boeing 737Max crash spoofed
- ■ NZ shooting incident
- ◆ NZ shooting incident spoofed

[F] IoT

Hacker intrusion

- ◆ Google Home
- ◆ Chromecast
- ◆ Smart TV
- ◆ Nest Camera

- ● EU published security standards "ETSI TS 103 645 V1.1.1" for IoT devices/products
- ○ Investigation of IoT vulnerabilities "NOTICE"

[G] Supply chain

- ■ PHP library PEAR
- ■ Debian APT
- ■ Ad-related SDK "RXDrioder" affecting more than 200 applications
- ASUS Live Update Utility affecting more than 1 million users ■

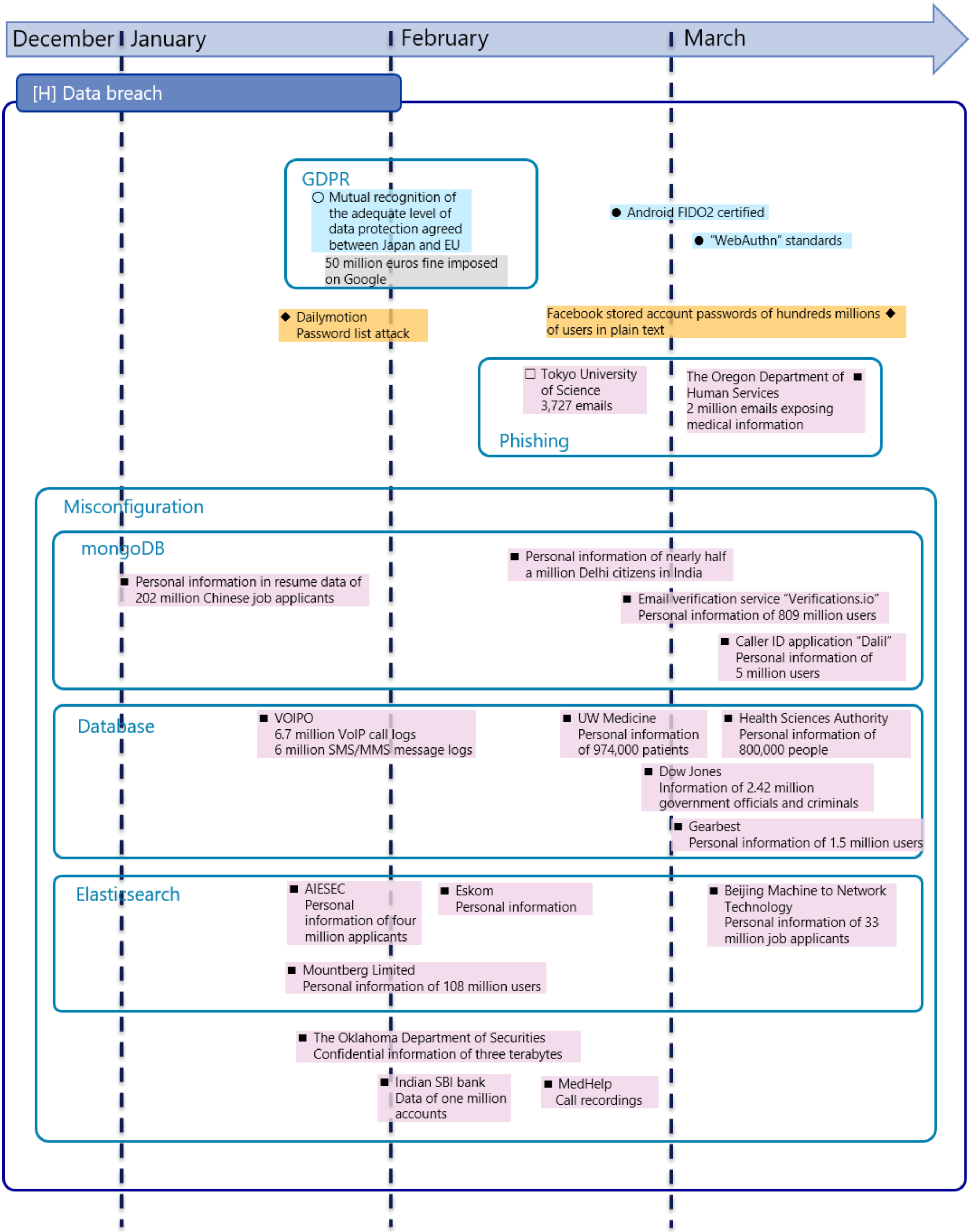
Timeline of 4th Quarter of 2018

*Some of the dates on the timeline are dates of article issuance
rather than dates of incident occurrence.

△□◇○:Domestic
▲■◆●:Global/Overseas

△▲:Vulnerability
□■:Incident

◇◆:Threat
○●:Measure



December | January | February | March

[H] Data breach

GDPR

○ Mutual recognition of the adequate level of data protection agreed between Japan and EU

50 million euros fine imposed on Google

● Android FIDO2 certified

● "WebAuthn" standards

◆ Dailymotion Password list attack

Facebook stored account passwords of hundreds millions of users in plain text ◆

Phishing

□ Tokyo University of Science 3,727 emails

The Oregon Department of Human Services 2 million emails exposing medical information ■

Misconfiguration

mongoDB

■ Personal information in resume data of 202 million Chinese job applicants

■ Personal information of nearly half a million Delhi citizens in India

■ Email verification service "Verifications.io" Personal information of 809 million users

■ Caller ID application "Dalil" Personal information of 5 million users

Database

■ VOIPO 6.7 million VoIP call logs 6 million SMS/MMS message logs

■ UW Medicine Personal information of 974,000 patients

■ Health Sciences Authority Personal information of 800,000 people

■ Dow Jones Information of 2.42 million government officials and criminals

■ Gearbest Personal information of 1.5 million users

Elasticsearch

■ AIESEC Personal information of four million applicants

■ Eskom Personal information

■ Beijing Machine to Network Technology Personal information of 33 million job applicants

■ Mountberg Limited Personal information of 108 million users

■ The Oklahoma Department of Securities Confidential information of three terabytes

■ Indian SBI bank Data of one million accounts

■ MedHelp Call recordings

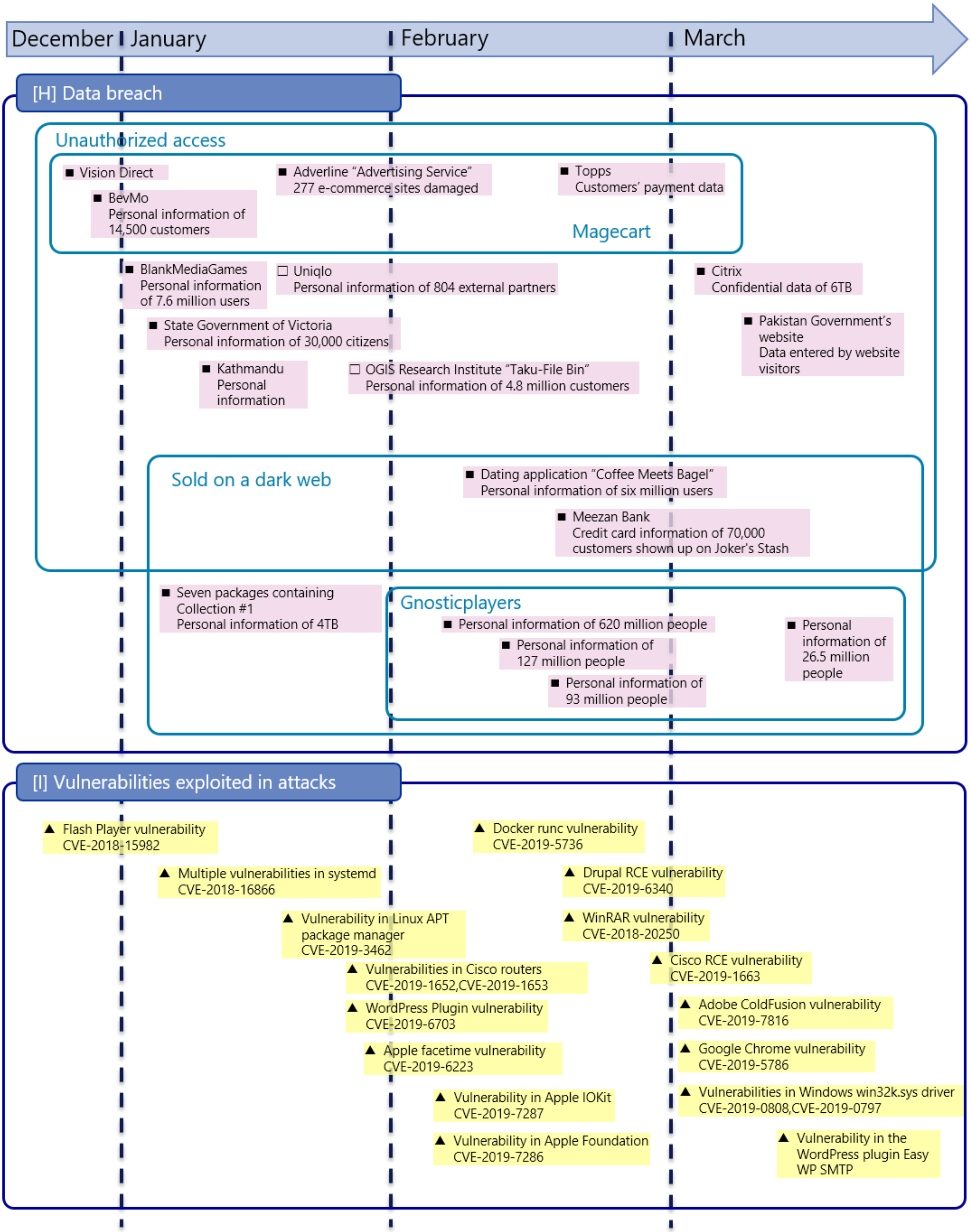
Timeline of 4th Quarter of 2018

*Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○:Domestic
▲■◆●:Global/Overseas

△▲:Vulnerability
□■:Incident

◇◆:Threat
○●:Measure



December | January | February | March

[H] Data breach

Unauthorized access

Magecart

- ■ Vision Direct
- ■ BevMo
  Personal information of 14,500 customers
- ■ Adverline "Advertising Service"
  277 e-commerce sites damaged
- ■ Topps
  Customers' payment data

- ■ BlankMediaGames
  Personal information of 7.6 million users
- □ Uniqlo
  Personal information of 804 external partners
- ■ Citrix
  Confidential data of 6TB
- ■ State Government of Victoria
  Personal information of 30,000 citizens
- ■ Pakistan Government's website
  Data entered by website visitors
- ■ Kathmandu
  Personal information
- □ OGIS Research Institute "Taku-File Bin"
  Personal information of 4.8 million customers

Sold on a dark web

- ■ Dating application "Coffee Meets Bagel"
  Personal information of six million users
- ■ Meezan Bank
  Credit card information of 70,000 customers shown up on Joker's Stash
- ■ Seven packages containing Collection #1
  Personal information of 4TB

Gnosticplayers

- ■ Personal information of 620 million people
- ■ Personal information of 127 million people
- ■ Personal information of 93 million people
- ■ Personal information of 26.5 million people

[I] Vulnerabilities exploited in attacks

- ▲ Flash Player vulnerability
  CVE-2018-15982
- ▲ Multiple vulnerabilities in systemd
  CVE-2018-16866
- ▲ Vulnerability in Linux APT package manager
  CVE-2019-3462
- ▲ Vulnerabilities in Cisco routers
  CVE-2019-1652,CVE-2019-1653
- ▲ WordPress Plugin vulnerability
  CVE-2019-6703
- ▲ Apple facetime vulnerability
  CVE-2019-6223
- ▲ Docker runc vulnerability
  CVE-2019-5736
- ▲ Drupal RCE vulnerability
  CVE-2019-6340
- ▲ WinRAR vulnerability
  CVE-2018-20250
- ▲ Vulnerability in Apple IOKit
  CVE-2019-7287
- ▲ Vulnerability in Apple Foundation
  CVE-2019-7286
- ▲ Cisco RCE vulnerability
  CVE-2019-1663
- ▲ Adobe ColdFusion vulnerability
  CVE-2019-7816
- ▲ Google Chrome vulnerability
  CVE-2019-5786
- ▲ Vulnerabilities in Windows win32k.sys driver
  CVE-2019-0808,CVE-2019-0797
- ▲ Vulnerability in the WordPress plugin Easy WP SMTP

References

[1] Barracuda Networks, Inc, "2019年以降のアプリケーションセキュリティトレンド," 14 3 2019. [Online]. Available: https://www.barracuda.co.jp/column/detail/964.

[2] NTT DATA Corporation, "グローバルセキュリティ動向四半期レポート(2018年度第2四半期)," 31 10 2018. [Online]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2018/2018103101/nttdata_fy2018_2q_securityreport.pdf.

[3] NTT DATA Corporation, "グローバルセキュリティ動向四半期レポート(2018年度第3四半期)," 13 2 2019. [Online]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_3q_securityreport.pdf.

[4] OXO International, Ltd., "Submitted Breach Notification," 3 1 2019. [Online]. Available: https://oag.ca.gov/system/files/OXO%20International%202%20Ad%20r2fin_0.pdf.

[5] L. Abrams, "OXO Breach Involved MageCart Attack That Targeted Customer Data," 7 1 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/oxo-breach-involved-magecart-attack-that-targeted-customer-data/.

[6] Trend Micro Incorporated, "New Magecart Attack Delivered Through Compromised Advertising Supply Chain," 16 1 2019. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.

[7] Sanguine Security, "Adminer leaks passwords; Magecart hackers rejoice," 17 1 2019. [Online]. Available: https://gwillem.gitlab.io/2019/01/17/adminer-4.6.2-file-disclosure-vulnerability/.

[8] Sanguine Security, "MySQL client allows MySQL server to request any local file," 20 1 2019. [Online]. Available: https://gwillem.gitlab.io/2019/01/20/sites-hacked-via-mysql-protocal-flaw/.

[9] The Topps Company, Inc., "NOTICE OF DATA BREACH," 22 2 2019. [Online]. Available: https://oag.ca.gov/system/files/CustomerNotice%28US%29%282.2019%29_0.pdf.

[10] P. Paganini, "Payment data of thousands of customers of UK and US online stores could have been compromised," 14 3 2019. [Online]. Available: https://securityaffairs.co/wordpress/82403/cyber-crime/payment-data-security-breach.html.

[11] Y. Klijnsma, "Consumers May Lose Sleep Over These Two New Magecart Breaches," 20 3 2019. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-mypillow-amerisleep/.

[12] RiskIQ, Inc, "Inside Magecart," 13 11 2018. [Online]. Available: https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf.

[13] Trend Micro Incorporated., "サイバー犯罪集団「Magecart」の新しい攻撃を確認、広告配信サービスを侵害しスキミングコードを注入," 18 1 2019. [Online]. Available: https://blog.trendmicro.co.jp/archives/20150.

[14] 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/.

[15] 独立行政法人情報処理推進機構, "情報セキュリティ10大脅威2019," 17 4 2019. [Online]. Available: https://www.ipa.go.jp/files/000072667.pdf.

[16] キヤノンマーケティングジャパン株式会社, "「Mac OS X」が生まれて16年——迫りつつあるマルウェアの脅威," 13 10 2017. [Online]. Available: https://eset-info.canon-its.jp/malware_info/trend/detail/171013.html.

[17] キヤノンマーケティングジャパン株式会社, "2017年9月 マルウェアレポート," 20 10 2017. [Online]. Available: https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1709.html#anc_02.

[18] PEAR, "PEAR公式Twitterアカウント," 19 1 2019. [Online]. Available: https://twitter.com/pear/status/1086634389465956352.

[19] M. Justicz, "Remote Code Execution in apt/apt-get," 22 1 2019. [Online]. Available: https://justi.cz/security/2019/01/22/apt-rce.html.

[20] Check Point Software Technologies LTD, "SimBad: A Rogue Adware Campaign On Google Play," 13 3 2019. [Online]. Available: https://research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/.

[21] AO Kaspersky Lab, "Operation ShadowHammer," 25 3 2019. [Online]. Available: https://securelist.com/operation-shadowhammer/89992/.

[22] AO Kaspersky Lab, "Kaspersky Lab、サプライチェーン攻撃手法を利用したAPT「ShadowHammer」を発見," 29 3 2019. [Online]. Available: https://www.kaspersky.co.jp/about/press-releases/2019_vir29032019.

[23] AO Kaspersky Lab, "Operation ShadowHammer: a high-profile supply chain attack," 23 4 2019. [Online]. Available: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/.

[24] GMO GlobalSign K.K., "二要素認証とは," [Online]. Available: https://jp.globalsign.com/service/clientcert/tfa.html.

[25] P. Duszyński, "Phishing NG. Bypassing 2FA with Modlishka.," 2 1 2019. [Online]. Available: https://blog.duszynski.eu/phishing-ng-bypassing-2fa-with-modlishka/.

[26] J. Cox, "Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts," 1 2 2019. [Online]. Available: https://www.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank.

[27] P. Duszyński, "GitHub - drk1wi/Modlishka: Modlishka. Reverse Proxy.," 31 1 2019. [Online]. Available: https://github.com/drk1wi/Modlishka/.

[28] P. Duszyński, "Phishing with Modlishka (bypass 2FA) on Vimeo," 29 12 2018. [Online]. Available:

https://vimeo.com/308709275.

[29] Security Affairs, “SS7 flaw allows hackers to spy on every conversation,” 15 8 2015. [Online]. Available: http://securityaffairs.co/wordpress/39409/cyber-crime/ss7-flaw-surveillance.html.

[30] Süddeutsche Zeitung Digitale Medien GmbH / Süddeutsche Zeitung GmbH, “Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer,” 3 5 2017. [Online]. Available: https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504.

[31] T. Hunt, “The 773 Million Record "Collection #1" Data Breach,” 17 1 2019. [Online]. Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/.

[32] K. o. Security, “773M Password ‘Megabreach’ is Years Old,” 17 1 2019. [Online]. Available: https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old/.

[33] RECORDED FUTURE, “Threat Actor Behind Collection #1 Data Breach Identified,” 1 2 2019. [Online]. Available: https://www.recordedfuture.com/collection-1-data-breach/.

[34] Soliton Systems, “約27億件の巨大漏洩ファイル「Collection#1」における日本の被害を特定,” 21 2 2019. [Online]. Available: https://www.soliton.co.jp/news/2019/003509.html.

[35] HackenProof, “No more privacy: 202 Million private resumes exposed,” 10 1 2019. [Online]. Available: https://blog.hackenproof.com/industry-news/202-million-private-resumes-exposed.

[36] ZDNet, “Online casino group leaks information on 108 million bets, including user details,” 21 1 2019. [Online]. Available: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/.

[37] オージス総研, “宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～,” 14 3 2019. [Online]. Available: 宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～.

[38] ZDNet, “ハッカーが約2カ月で10億件に迫るユーザー情報をダークウェブで公開の恐れ,” 16 4 2019. [Online]. Available: https://japan.zdnet.com/article/35135809/.

[39] B. DIACHENKO, “800+ Million Emails Leaked Online by Email Verification Service,” 7 3 2019. [Online]. Available: https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service/.

[40] Citrix, “Citrix provides update on unauthorized internal network access,” 4 4 2019. [Online]. Available: https://www.citrix.com/blogs/2019/04/04/citrix-provides-update-on-unauthorized-internal-network-access/.

[41] C. P. Research, “Extracting a 19 Year Old Code Execution from WinRAR,” 20 2 2019. [Online]. Available: https://research.checkpoint.com/extracting-code-execution-from-winrar/.

[42] 360威胁情报中心, “Warning! Upgrades in WinRAR Exploit with Social Engineering and Encryption,” 27 2 2019. [Online]. Available: https://ti.360.net/blog/articles/upgrades-in-winrar-exploit-with-social-

engineering-and-encryption/.

[43] tenable, "Multiple Zero-Day Vulnerabilities Discovered by Tenable Research in Building Access Technology," 14 1 2019. [Online]. Available: https://www.tenable.com/press-releases/multiple-zero-day-vulnerabilities-discovered-by-tenable-research-in-building-access.

[44] TechCrunch, "Researcher shows how popular app ES File Explorer exposes Android device data," 16 1 2019. [Online]. Available: https://techcrunch.com/2019/01/16/android-app-es-file-explorer-expose-data/.

[45] BAD PACKETS REPORT, "Over 9,000 Cisco RV320/RV325 routers are vulnerable to CVE-2019-1653," 26 1 2019. [Online]. Available: https://badpackets.net/over-9000-cisco-rv320-rv325-routers-vulnerable-to-cve-2019-1653/.

[46] Defiant, "WordPress Sites Compromised via Zero-Day Vulnerabilities in Total Donations Plugin," 25 1 2019. [Online]. Available: https://www.wordfence.com/blog/2019/01/wordpress-sites-compromised-via-zero-day-vulnerabilities-in-total-donations-plugin/.

[47] Apple, "About the security content of iOS 12.1.4 - Apple Support," 7 2 2019. [Online]. Available: https://support.apple.com/en-us/HT209520.

[48] Google Project Zero, "1726 - XNU_ copy-on-write behavior bypass via mount of user-owned filesystem image - project-zero - Monorail," 1 12 2018. [Online]. Available: https://bugs.chromium.org/p/project-zero/issues/detail?id=1726&q=.

[49] ZDNet, "Doomsday Docker security hole uncovered," 11 2 2019. [Online]. Available: https://www.zdnet.com/article/doomsday-docker-security-hole-uncovered/.

[50] LAC, "【注意喚起】CMSのDrupal 、RCEで危険度の高い脆弱性(CVE-2019-6340)。至急、最新版への更新を," 25 2 2019. [Online]. Available: https://www.lac.co.jp/lacwatch/alert/20190225_001779.html.

[51] Adobe, "Security updates available for ColdFusion | APSB19-14," 1 3 2019. [Online]. Available: https://helpx.adobe.com/security/products/coldfusion/apsb19-14.html.

[52] Google, "Stable Channel Update for Desktop," 1 3 2019. [Online]. Available: https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html.

[53] tenable, "Use-After-Free Vulnerability in Google Chrome Exploited In The Wild (CVE-2019-5786)," 6 3 2019. [Online]. Available: https://www.tenable.com/blog/use-after-free-vulnerability-in-google-chrome-exploited-in-the-wild-cve-2019-5786.

[54] Microsoft, "CVE-2019-0797 | Win32k Elevation of Privilege Vulnerability," 12 3 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0797.

[55] Microsoft, "CVE-2019-0808 | Win32k Elevation of Privilege Vulnerability," 12 3 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0808.

[56] Melon Security, "Emotet: A Small Change in Tactics Leads to a Spike in Attacks," 12 2 2019. [Online]. Available: https://www.menlosecurity.com/blog/emotet-a-small-change-in-tactics-leads-to-a-spike-

in-attacks.

[57] Check Point Research, "SpeakUp: A New Undetected Backdoor Linux Trojan," 4 2 2019. [Online]. Available: https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/.

[58] Cisco Talos, "Cisco AMP tracks new campaign that delivers Ursnif," 24 1 2019. [Online]. Available: https://blog.talosintelligence.com/2019/01/amp-tracks-ursnif.html.

[59] Trend Micro Incorporated, "「顔文字」、「LoveYou」スパムの背後に凶悪スパムボット、ランサムウェア遠隔攻撃も実行," 22 2 2019. [Online]. Available: https://blog.trendmicro.co.jp/archives/20392.

[60] BLEEPING COMPUTER, "New Astaroth Trojan Variant Exploits Anti-Malware Software to Steal Info," 13 2 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-astaroth-trojan-variant-exploits-anti-malware-software-to-steal-info/.

[61] Carbon Black, "TAU Threat Intelligence Notification: New macOS Malware Variant of Shlayer (OSX) Discovered," 12 2 2019. [Online]. Available: https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/.

[62] TG Soft, "21/02/2019 14:48:47 - Operazione Pistacchietto: Spyware italiano attivo dal 2016 si diffonde attraverso la piattaforma di GitHub," 21 2 2019. [Online]. Available: https://www.tgsoft.it/italy/news_archivio.asp?id=987.

[63] McAfee, "Happy New Year 2019! Anatova is here!," 22 1 2019. [Online]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/happy-new-year-2019-anatova-is-here/.

[64] BLEEPING COMPUTER, "Jokeroo Ransomware-as-a-Service Offers Multiple Membership Packages," 5 3 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/jokeroo-ransomware-as-a-service-offers-multiple-membership-packages/.

[65] BLEEPING COMPUTER, "CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers," 5 3 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/.

[66] BLEEPING COMPUTER, "JNEC.a Ransomware Spread by WinRAR Ace Exploit," 18 3 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/jneca-ransomware-spread-by-winrar-ace-exploit/.

[67] BLEEPING COMPUTER, "Yatron Ransomware Plans to Spread Using EternalBlue NSA Exploits," 12 3 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/yatron-ransomware-plans-to-spread-using-eternalblue-nsa-exploits/.

[68] Trend Micro, "暗号化型ランサムウェア「LockerGoga」について解説," 8 4 2019. [Online]. Available: https://blog.trendmicro.co.jp/archives/20840.

[69] BLEEPING COMPUTER, "GandCrab Operators Use Vidar Infostealer as a Forerunner," 7 1 2019.

[Online]. Available: https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/.

[70] Unit 42, “Mac Malware Steals Cryptocurrency Exchanges’ Cookies,” 31 1 2019. [Online]. Available: https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/?fbclid=IwAR1q6bzf0Mz_9vyzRUMH6irpNGaKXN3n2A00F1nP11AL6YTFrh57zUg9Z-I.

[71] avast, “Spoofing in the reeds with Rietspoof,” 19 2 2019. [Online]. Available: https://blog.avast.com/rietspoof-malware-increases-activity.

[72] Trend Micro Incorporated, “「Trickbot」がリモートデスクトップアプリの認証情報を窃取する機能を追加,” 18 2 2019. [Online]. Available: https://blog.trendmicro.co.jp/archives/20375.

[73] Trend Micro, “サイネージTVとプレゼンテーションシステムを狙う「Mirai」の新しい亜種を確認,” 26 3 2019. [Online]. Available: https://blog.trendmicro.co.jp/archives/20709.

[74] Kaspersky Lab, “ATM robber WinPot: a slot machine instead of cutlets,” 19 2 2019. [Online]. Available: https://securelist.com/atm-robber-winpot/89611/?utm_source=kdaily&utm_medium=blog&utm_campaign=jp_kd_Ex0124_organic&utm_content=link&utm_term=jp_kdaily_organic_Ex0124_link_blog_kd.

[75] U.S. Department of Defense, “DARPA Explores New Computing Architectures to Deliver Verifiable Data Assurances,” 16 1 2019. [Online]. Available: https://www.darpa.mil/news-events/2019-01-16.

[76] American Institute of Physics, “Office of Critical Technologies and Security Act - H.R.618 / S.29,” 16 1 2019. [Online]. Available: https://www.aip.org/fyi/federal-science-bill-tracker/116th/office-critical-technologies-and-security-act.

[77] U.S. Department of Justice, “Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers,” 30 1 2019. [Online]. Available: https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north.

[78] delmarva now., “Ransomware attacks would become felony with Maryland bill,” 15 2 2019. [Online]. Available: https://www.delmarvanow.com/story/news/local/maryland/2019/02/15/ransomware-attacks-would-become-felony-maryland-bill/2869037002/.

[79] National Institute of Information and Communications Technology, “IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施,” 1 2 2019. [Online]. Available: https://www.nict.go.jp/press/2019/02/01-1.html.

[80] BBC., “Russia bans smartphones for soldiers over social media fears,” 20 2 2019. [Online]. Available: https://www.bbc.com/news/world-europe-47302938.

[81] E Hacking News., “Soon DNS to protect users from malware,” 24 2 2019. [Online]. Available: https://www.ehackingnews.com/2019/02/soon-dns-to-protect-users-from-malware.html.

[82] European Union Agency for Law, “Law enforcement agencies across the EU prepare for major cross-

border cyber-attacks," 18 3 2019. [Online]. Available: https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks.

[83] National Institute of Standards and Technology, "Security Strategies for Microservices-based Application Systems: Draft NIST SP 800-204 Available for Comment," 25 3 2019. [Online]. Available: https://csrc.nist.gov/news/2019/nist-releases-draft-sp-800-204-for-public-comment.

[84] International Association of Privacy Professionals., "First GDPR fine in Portugal issued against hospital for three violations," 3 1 2019. [Online]. Available: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

[85] Commission Nationale de l'Informatique et des Libertés, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC," 21 1 2019. [Online]. Available: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[86] Personal Information Protection Commission, Government of Japan., "日EU間の相互の円滑な個人データ移転を図る枠組み発効," 23 1 2019. [Online]. Available: https://www.ppc.go.jp/enforcement/cooperation/cooperation/310123/.

[87] CBS Interactive Inc., "Google appeals $57M GDPR fine, defends privacy practices," 24 1 2019. [Online]. Available: https://www.cnet.com/news/google-appeals-57m-gdpr-fine-defends-privacy-practices/.

[88] European Commission, "Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel ahead of Data Protection Day," 25 1 2019. [Online]. Available: http://europa.eu/rapid/press-release_STATEMENT-19-662_en.htm.

[89] Dutch Data Protection Authority, "Websites moeten toegankelijk blijven bij weigeren tracking cookies," 7 3 2019. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies.

[90] The President of the Personal Data Protection Office, "The first fine imposed by the President of the Personal Data Protection Office," 26 3 2019. [Online]. Available: https://uodo.gov.pl/en/553/1009.

[91] Verizon Media, "Cookie walls don't comply with GDPR, says Dutch DPA," 8 3 2019. [Online]. Available: https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/.

[92] Bisnode Polska sp. z. o.o., "Decision of UODO (Polish DPA) - Bisnode statement," [Online]. Available: https://www.bisnode.pl/wiedza/newsy-artykuly/decyzja-urzedu-ochrony-danych-osobowych-w-sprawie-bisnode/.

May 30, 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