NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends (3rd Quarter of 2018)

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department

Table of Contents

1. Executive Summary

There were several Data breach incidents, which attracted public attention. Examples of incidents especially remarkable were information leak of 29 million people from Facebook at the end of September and customer information leak of 500 million people announced by Marriott in November. Some of large web service operators, called platformers, have hundreds of millions of users, and thus, tend to pose significant damage once a security incident happens. Service users should exercise their information literacy by, for example, selecting an appropriate service operator, filtering the information to be registered to services rather than thoughtlessly entrusting information and resources, and grasping what information they have registered.

From the previous quarter, fraud and phishing incidents related to web and cloud services continue to be prevalent. Attackers steal money and passwords by fraud and phishing techniques. They earn a lot if they succeed in such an attack. Email remains the main means of fraud, but incidents using other media such as SMS and social media are increasing. For example, IPA[1] announced that cases on fraud SMS messages disguised as Sagawa Express rose from 24 of September to 169 in October and 182 in November. Some message texts smartly took advantage of a disaster or a carrier trouble.

As for attacks on cryptocurrencies, there are increasing mining attacks that abuse servers, routers, IoT devices, and other devices that automatically run for extended periods. It is difficult to notice high CPU consumption caused by mining on these devices, and therefore, the detection of unlawful mining tends to delay. Basic measures are effective such as applying patches for vulnerabilities and setting a strong password to prevent unauthorized access.

As a trend in attacks on service user, there are supply chain attacks that exploit open-source software. There was a case of distributing a software development kit (SDK) containing a malicious code. Software and services that were developed by the SDK had a backdoor and a mining program, and using them resulted in mining and hijack. Individuals and corporations must be careful of supply chain attacks like this one when they develop software using an open-source development environment.

If the market prices of cryptocurrencies drop in the future, making it difficult to profit from unlawful mining, attackers may turn resources from cryptocurrency attacks to different types of attacks.

[1] Information-technology Promotion Agency, Japan

2. Topics in 3rd quarter of 2018

2.1. Data breach, personal information, and privacy

About Facebook, a number of information leak incidents were reported including the theft of 29 million tokens by exploiting the vulnerability of the "View As" function [1], the theft and trade of 81 thousand pieces of personal data through the abuse of an extended function of a web browser [2], and a software bug which might well have caused the leak of photographs to external application developers [3]. Facebook attracted attention from the viewpoint of administration and regulations in different countries—the Personal Information Protection Committee of Japan issued an administrative direction on personal information leak including the incident of Cambridge Analytica [4], and ICO of UK incurred a 500 thousand pound fine on a violation of data protection regulations [5].

Table 1: Incidents related to Facebook Data breach

Date	Overview	Damage quantity
September 28th	Facebook announced that it received a cyber attack that stole a maximum of 50 million tokens usable for account login and it reset tokens of 90 million users. The attacker exploited the vulnerability of the "View As" function, which is used for checking profiles [6].	50 million
October 12th	Facebook announced that 29 million users were damaged through the theft of 50-million-user tokens at a maximum. According to the report, the attacker viewed the important information of 14 million users among 29 million [1].	29 million (corrected)
October 22nd	The Personal Information Protection Committee of Japan administration announced that it issued an administrative direction to Facebook. There were three subjects of the administrative direction: a social plug-in that automatically sends information, the incident of Cambridge Analytica, and information leak through the abuse of the "View As" function [4].	None
October 24th	The Information Commissioner's Office (ICO), which is the personal information protection authority in UK, executed the plan of issuing a fine of 500 thousand pounds to Facebook about the incident of user data collection. It claims improper handling of data regarding over a million users in UK. [5].	None
November 2nd	BCC reported that the personal data of 81 thousand accounts were stolen and sold. In a network forum of English-speaking users, a user by the name of "FBSaler" announced that it would sell account information and posted sample profile data of over 81 thousand users to the forum. Facebook claims that it is a lawful data collected by a browser extension, and therefore, the data breach does not constitute a fault of Facebook [2].	81 thousand
December 14th	Facebook announced that images in smartphones might well have leaked to external application developers due to a software bug. A maximum of 6.8 million users were in a vulnerable situation. [3]	6.8 million

Other reported incidents include personal information leak of a maximum of 500 thousand Google+ accounts and a large-scale information leak from the world's largest hotel group, Marriott, through unauthorized access. Marriott announces that this data braech incident impacts 500 million customers who made reservations from Starwood Hotels and Resorts Worldwide. Prompted by an alarm on attempts of unauthorized database access raised by an internal security tool on September 8th, 2018, Marriott investigated and found that unauthorized access started in 2014. The company offers to affected users one-year free subscription of "WebWatcher", an external service that monitors personal information leak.

Table 2: Incidents related to data breach

Date	Overview	Damage quantity
October 8th	Google announced that personal information of a maximum of 500 thousand Google+ accounts leaked due to an API defect. Google plans to terminate the Google+ service [7].	500 thousand
October 9th	An attacking group "Magecart" attacked a plug-in "review widget" of Shopper Approved. "Review widget" is a plug-in used by online shop customers to rate products [8].	Not announced
October 13th	Associated Press reported that the US Defense Department suffered an infringement caused by a third-party contractor, which affected 30 thousand military or civilian staff [9].	30 thousand
October 24th	Cathay Pacific Airways announced that it encountered an attack, and the data of 9.4 million passengers might be affected at a maximum. Leaked information includes passport numbers, identity card numbers, email addresses, and credit card numbers [10].	9.4 million
November 6th	"Anonymous" of Italy leaked new information. Exposed documents contained the personal information of the national research council of Italy, The Equitalia's Database, and employees and related people of research institutions of the ministry of economic development [11].	Not announced
November 8th	A credit card company, American Express India, exposed an unsecured MongoDB server online. The server contained the information of 700 thousand customers [12].	700 thousand
November 14th	The online store of Infowars, the website of a radio show host Alex Jones, encountered a credit card skimming attack committed by attacking group Magecart [13].	Not announced
November 22nd	The account information of 60 million people of the US postal service was reported to have been viewable for a year [14].	60 million
November 30th	Marriott, a large hotel company, announced that there had been unauthorized access to the reservation database of its subsidiary, Starwood, from 2014. Personal information of a maximum of 500 million people is vulnerable to infringement [15].	500 million

Many businesses collect personal information of users. On the other hand, there were incidents of collecting and trading personal information while users are not aware.

Table 3 Incidents of collecting and trading personal information

Date	Overview
October 9th	B9 Systems announced the result of an investigation on the handling of personal information in health-care websites. The investigated websites shared personal information with 57 external sites on average, which included advertisement, marketing, and social media sites [16].
October 18th	The Ministry of Internal Affairs and Communications, Japan held the first study meeting to discuss how big IT companies such as GAFA[2] should be regulated. Because these platformers are overseas companies, to which Telecommunications Business Act does not apply, there has been concern on the handling of personal information [17].
October 18th	A researcher of University of Oxford downloaded about 960 thousand applications from the Google Play Store to see whether they had third party trackers. The median count of trackers included in each application was 10, and 90% of the applications included at least one tracker [18].
December 10th	Location information of users collected by a free Android application was found to be sold to an advertising company. This application, GasBuddy, has functions such as showing routes to gas stations. The advertising company that bought the location information was Reveal Mobile. The price of the information was $9.5 per 1000 users [19].

2.2. Phishing scam

2.2.1. Phishing incidents increasing in Japan

Phishing techniques in Japan are becoming more sophisticated. In November, IPA called attention to a new technique that uses false short messages that were disguised as courier companies [20]. IPA said that there was a sharp increase in consultations on phishing incidents disguised as courier companies in July 2018 and also in October and November (see Figure 1). Phishing sites that attempt to install bad applications are increasing not only for Android devices but also for iOS devices. Some of the new techniques include those that use a SMS message that contain a URL to direct the user to a false site that is disguised as a real site (see Figure 2 and Figure 3). This type of phishing techniques are increasing, including those disguised as Sagawa Express or Yamato Transport.

December 2018 had a sharp increase of fraud emails, and many different kinds of fraud emails are reported. Japan Cybercrime Control Center reports fraud emails that are disguised as Amazon or Rakuten, business fraud emails that are disguised as invoices and delivery slips, blackmail emails in which the sender claims that they stole a password, and so forth [21].

[2] GAFA is the acronym of Google, Apple, Facebook, and Amazon.

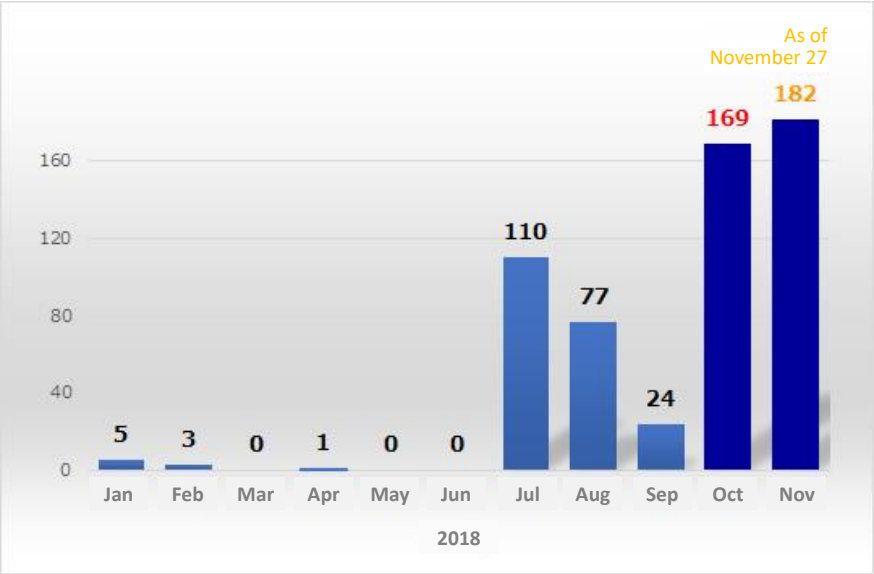


Figure 1: Cases reported to IPA about "SMS disguised as Sagawa Express" in 2018 [20]

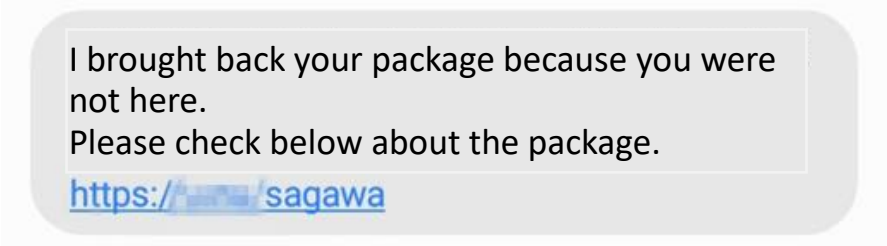


Figure 2: Example of phishing SMS message disguised as notification of delivery in absence [22]

Figure 3: Example of authentic false site (left: false site, right: real site) [23]

2.2.2. Sophistication of phishing techniques overseas

A new phishing technique is reported. Netskope Threat Protection reported a phishing technique in October 3rd, in which the attacker let the user open a PDF file stored in Google Drive. When the user opens the PDF file, a phishing page of Office 365 appears that is stored on an Azure BLOB storage linked from the PDF file. The Azure BLOB storage has a domain and an SSL certificate issued by Microsoft allowing the browser to connect with SSL (see Figure 4). The user mistakenly considers it as an official website connected with SSL [24].

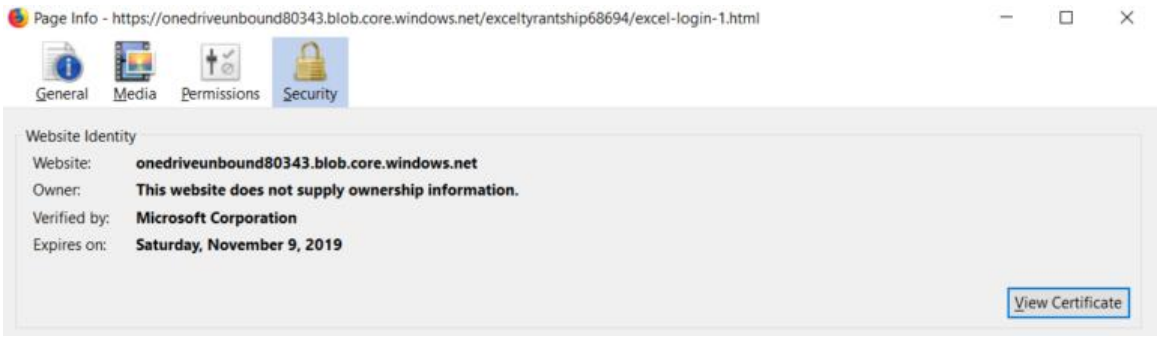


Figure 4: Example of phishing site protected by Microsoft SSL certificate

Bleeping Computer reports another fact about this phishing scam: the attacker uses the IPFS gateway service to access the InterPlanetary File System (IPFS), which is a P2P file system provided by a CDN service company, CloudFlare [25]. CloudFlare released the IPFS gateway service in September. All connections to the IPFS gateway service are protected by an SSL certificate issued by CloudFlare. Therefore, the attacker can exploit HTTP access protected by an SSL certificate issued by CloudFlare to convince the user that they are filling out an entry form of an official site.

Other than Azure BLOB storage, fraud incidents that use the Google Cloud Storage service are also identified. Menlo Labs reports the result of tracking a malicious email campaign that targets employees of banks and financial service companies. The attacker let the victim click a malicious link written in an email for access to a file stored in storage.googleapis.com, which is the domain of the Google Cloud Storage service [26].

According to the December report of PhishLabs, 49.9% of all phishing sites use SSL certificates. PhishLabs reports, "Although SSL certificates of phishing sites do not prove the legitimacy of the sites, users are deceived by the padlock mark on Chrome or Internet Explorer into considering that they are accessing official sites [27]."

As explained above, one cannot determine whether a website is an official site or a phishing site only by the presence/absence of an SSL certificate. If a user attempts to access a website and the actual destination is a cloud service domain such as Azure BLOB or Google Cloud Storage, the user should suspect a phishing site. Attackers use sophisticated phishing techniques as explained above because web browsers have implemented the function of raising an alarm when the user accesses a website without SSL authentication.

2.3. Attacks targeting cryptocurrencies

Table 4 categorizes attack methods that target cryptocurrencies, by cryptocurrency trades and targeted victims. This report categorizes attacks by targeted victims.

Table 4 : Categorization of attack methods targeting cryptocurrencies

Cryptocurrency trade	Targeted victim	Description/example of attack
Traders of cryptocurrencies	Providers of cryptocurrency services	Attacks targeting wallets of a cryptocurrency exchange
Not related to cryptocurrency trade	Users of cryptocurrency services	Attacks that steal authentication information used for login to a cryptocurrency exchange
	Computer owners	Attacks that infect cryptocurrency miners, drive-by mining, etc.

2.3.1. Attacks targeting cryptocurrency service providers

Attacks targeting cryptocurrency service providers decreased in October to December 2018 compared to the previous quarter (July to September). There was an insider attack targeting cold wallets. This attack was a rare one, disguised as an external attack. There are two types of cryptocurrency wallets: hot wallets and cold wallets. Hot wallets are managed with Internet connection, while cold wallets are managed without Internet connection. Therefore, cold wallets are considered secure against hacking. In a past report "Quarterly Report on Global Trend on Cybersecurity", we advocated transfer from hot wallets to cold wallets as an example of countermeasures against hacking. In view of these facts, users of cryptocurrency services must be wary when selecting an exchange.

Table 5: List of attacks targeting cryptocurrency service providers

Date	Overview of attack	Damage
October 21st	TIO 50 million was stolen by hacking from a cryptocurrency exchange in Switzerland, Trade.io. The total damage is about $11 million. This case attracted public attention as an incident targeting cold wallets. The criminal is considered to be a person that has physical access to cold wallets [28].	$11 million
October 28th	A cryptocurrency exchange in Canada, Maplechange, lost all BTC by hacking. The amount lost is 913 BTC, which accounts for about $6 million. The official site was closed and SNS data was erased. There is a suspicion that this incident is a forgery, not a fraud [29].	$6 million

2.3.2. Attacks targeting cryptocurrency service users

An analyst of Doctor Web provided an investigation report on a wide range of malware and attacking methods used by an attacker named Investimer. According to the report, Investimer uses not only commercially available trojan malware but also malware of a spy-agent backdoor that exploits TeamViewer, DarkVNC and HVNC backdoors for access to computers by the VNC protocol, an RMS-based backdoor, and so forth. The report also says that the managing servers are installed in official websites of telecommunications company services and hosting services such as jino.ru, marosnet.ru, and hostlife.net, and the attacker has deployed many phishing sites targeting Dogecoin [30].

There have been incidents of malicious codes installed in most-used websites and OSS for the theft of cryptocurrency [31] [32]. Everyone can get source codes from OSS and change them, so that they might be modified to a malicious code. It is difficult to notice a malicious code embedded in OSS than to find that a website

is falsified. Especially, software developers and businesses must be wary of supply chain attacks that exploit open-source development environment (SDK: Software Development Kit). There was a case of developing software using an open-source development environment provided by an attacker with a malicious code. The developed software contained a backdoor and a mining program, so that users of the software suffered mining and hijack. Developers should get OSS from a trusted website. Developers should also check the source and developer of the open-source development environment before using it to confirm that it has not been modified. The source and developer of an open-source development environment rarely change. If they are changed, the open-source development environment might be bought by an attacker who uses it as attacking means. Do not use a suspicious development environment that might be provided by an attacker. People who use OSS must know these risks and evaluate the risk of using it by themselves.

There was an attack in a foreign country that stole web wallet accounts using a method called SIM swapping [33]. SIM swapping is the act of hijacking a phone number. One method of SIM swapping is to retrieve the encrypted phone number ID from the subscriber identity module (SIM) of a mobile phone and copy it to the SIM of another mobile phone.

In an incident of November, the attacker contacted the customer service to change the SIM of a mobile phone of a certain person, and linked the phone number of the person to a new mobile phone that attacker prepared. Next, the attacker requested to change the password of a web wallet account of a cryptocurrency, and passed two-factor authentication using that mobile phone to succeed in changing the password. The attacker used the modified password to log in to the cryptocurrency web wallet of the person to retrieve cryptocurrency. Cryptocurrency worth of $1 million was stolen in a short period before the victim found something unusual on the mobile phone and contacted the provider. The victim is a big name of Silicon Valley, so this attack was a targeted attack that targets a certain rich person.

Table 6: List of attacks targeting cryptocurrencies of cryptocurrency service users

Date	Overview of attack
November 8th	ESET found a malicious code that is considered to be inserted by an attacker who compromised an online web analysis platform named StatCounter. The code can hijack any bit coin transactions executed through the web interface of a cryptocurrency exchange, Gate.io [31].
November 22nd	A 21-year-old attacker was reported to have stolen cryptocurrency valued at about $1 million using a method called SIM swapping. The attacker stole the phone number of the victim by contacting customer service and pretending to change the SIM [34].
November 27th	A JavaScript library, Event-Stream, was reported to have an embedded code for stealing coins from cryptocurrency wallets [32].
November 28th	The Nagoya District Public Prosecutors Office sent an 18-year-old person to the Nagoya Family Court on the creation and sharing of an illegal instruction electromagnetic record. The prosecuted person made a computer virus to unlawfully get cryptocurrency of Monacoin [35].

2.3.3. Attacks targeting computing resources of computers

Mining malware, which mine cryptocurrencies, are still active. You should be wary of them even if you do not use cryptocurrencies. In December, McAfee reported that there was a sharp increase of mining malware in the previous quarter (July to September 2018) [36]. The scope of their impact is extensive because they target computing resources of computers. It is necessary to watch out them in the future.

Table 7 : List of attacks targeting computing resources of computers

Date	Overview of attack
October 11th	A researcher, Brad Duncan, found a new method in which the attacker installs mining malware by disguised as an update of Adobe Flash Player. The new thing about this method is the use of an update of Adobe Flash Player to reduce a sense of distrust that users may have [37].
October 22nd	The National Police Agency, Japan called attention to attacks targeting Android devices that have ADB debugging enabled [38]. There have been reports and alarms on this vulnerability from JVN [39], and on attacks targeting TCP port 5555 used by ADB from the National Police Agency, Japan [39]. The communication destined to TCP port 5555 is used to download and install mining malware.
October 25th	Trend Micro found an attack that uses the Docker Engine API for cryptocurrency mining. The misuse of the Docker Engine API has been considered problematic since before, but there are still improperly configured Docker Engines allowing attacks to continue [40].
November 1st	St. Francis Xavier University suffered an attack called cryptcoin mining, and the university shut off its network. As a countermeasure, the university reset all passwords. The evidence of personal information infringement had not been found at the time of the report [41].
November 12th	McAfee Labs found a new Russian malware called WebCobra, which exploits victims' computers to perform cryptocurrency mining. The unique thing about this method is that it installs different miners in accordance with the configuration of the target device [42].
November 19th	An international non-profitable organization, Make-A-Wish Foundation, found that its website (worldwish.org) was compromised and was installed with a JavaScript mining program, CoinIMP, which mines cryptocurrency Monero [43].

2.4. Conflict between the U.S. and China

2.4.1. Incident related to microchip of Super Micro

A US media, Bloomberg Businessweek, featured an article "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" on October 4th, 2018 [44]. The article claims that motherboards of Super Micro, which are manufactured in China and used in the U.S., have a microchip smaller than a grain of rice, and that China used the microchip to access intellectual properties and confidential information of the United States. This article attracted tremendous attention involving Apple, Amazon, and many countries in the world.

Table 8: Incident related to microchip of Super Micro

Date	Overview of attack
October 4th	Bloomberg Businessweek featured an article "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", which claims that motherboards of Super Micro have a microchip that provides access to information [44].
October 4th	Amazon, Apple, and Super Micro expressed dissenting views by an email statement against the summary of the Bloomberg Businessweek report [45].
October 4th	Amazon pronounced a negative statement against the Bloomberg BusinessWeek article on the microchip of Super Micro. It claimed that no hardware problem had been found and it had engaged in no investigation with the government [46].
October 5th	National Cyber Security Center (NCSC) under the umbrella of Government Communications Headquarters (GCHQ, information agency of the UK) announced its view that there was no evidence against Apple and Amazon's claims that repudiated the Bloomberg BusinessWeek article [47].

Date	Overview of attack
October 8th	George Stathakopoulos, Apple vice-president responsible for information security, sent a message to the Congress that strongly repudiates the article. He says, "We have not found any malicious chip, hardware falsification, or intentionally created vulnerability in any server." [48]
November 2nd	A US Senate Committee requested FBI and Department of Homeland Security a confidential explanation on the report that claims the China intelligence agency made a subcontractor implant malicious chips on server motherboards of Super Micro. Department of Homeland Security stated that there was no reason for doubting the opinions of the companies that repudiate the Bloomberg Businessweek report [49].
December 11th	In a disclosed letter sent to customers, Super Micro Computer reported the result of an investigation conducted by a research company. The report said that there was no evidence supporting the article that claims malicious hardware was implanted in the motherboard of Super Micro Computer [50].

2.4.2. Incidents related to Huawei

According to the report of the Wall Street Journal, the US government requested its allies including Japan, Germany, and Italy not to use Huawei products because they pose cyber security risks [51]. Afterwards, governments and major telecommunication companies announced their statements, attracting public attention.

Table 9: Incidents related to Huawei

Date	Overview of attack
November 23rd	According to the report of the Wall Street Journal, the US government requested its allies including Japan, Germany, and Italy not to use Huawei products because they pose cyber security risks [51].
November 28th	The intelligence agency of New Zealand rejected the request of "using 5G devices of Huawei" for the first time in the telecommunications industry of the nation for the concern of national security [52].
December 5th	The government of Canada arrested the CFO of Huawei, Wanzhou Meng, in Vancouver responding to the request of the United States. She is suspected of violating a US sanction against trade with Iran. Huawei announced a statement that it did not have information on the charge and did not identify any negligence by Wanzhou Meng [53].
December 5th	BT, a major telecommunications company of the UK, announced that it would eliminate Huawei products from existing 3G and 4G core networks and would not use them as major components of the 5G network [54].
December 7th	The government of Germany indicated its policy of not excluding any manufactures or high-tech companies for the deployment of 5G network. This policy was announced by the spokesperson of Ministry of Home Affairs [55].
December 10th	The government of Japan announced its decision of excluding Huawei and ZTE products from government procurement in "Policy on the procurement of information and communication equipment used by the central government and the Self-Defense Forces" [56].
December 14th	Deutsche Telekom has had the strategy of procuring from multiple vendors with major vendors of Ericsson, Nokia, Cisco, and Huawei. However, it announced that it was reconsidering this strategy [57].
December 14th	Orange, a major telecommunications company in France, announced its policy of not using Huawei products in the deployment of the 5G network [57].

2.5. Vulnerabilities, and attacks that exploit them

2.5.1. Zero-day attacks

A zero-day attack is an attack that exploits a software security vulnerability that an attacker finds before the vulnerability is widely publicized. In this quarter, there were zero-day attacks on Microsoft and Adobe products. Because of the big impact of zero-day attacks and many users of Microsoft and Adobe products, the manufacturers and public institutions urged the users for the quick application of security update programs.

Table 10 Zero-day attack incidents

Date	Product	Vulnerability number	Overview
October 9th	Windows	CVE-2018-8453	Microsoft released a security update for vulnerabilities of Windows. Among the vulnerabilities, Microsoft announced that it identified an exploitation of CVE-2018-8453 [58]. According to Kaspersky, this vulnerability was used in a targeted attack aiming at the Middle East region in August [59].
October 23rd	Windows	-	A Twitter user by the name of SandboxEscaper publicized a vulnerability of Windows privilege escalation with a PoC code (see Figure 5). The same Twitter user also publicized a privilege elevation vulnerability in the Windows task scheduler in August [60] [61].
October 31st	Cisco ASA	CVE-2018-15454	Cisco reported a DoS vulnerability in the SIP protocol of Cisco ASA and Cisco FTD. Cisco said that it found a fraudulent SIP messages that exploited the vulnerability, and called for the application of a mitigation measure. The company released an updated software version that had a correction of the vulnerability on November 6th or later [62].
November 8th	VirtualBox	-	A security researcher, Sergey Zelenyuk, publicized a vulnerability and a PoC code regarding privilege escalation related to virtual NICs of VirtualBox. He did not make an advance notification to the vendor (Oracle) about the publication. The researcher says that he raised the problem because of the half-year waiting period for vulnerability fix and his dissatisfaction on the bug reward system [63].
November 6th	WordPress	CVE-2018-19207	A privilege escalation vulnerability was found in WP GDPR Compliance, which is a WordPress plug-in. An attacker exploited this vulnerability to install a backdoor program in multiple sites [64] (see Figure 6). In response to this report, the plug-in developer released an updated software version that had an update for the vulnerability on November 7 [65].
November 13th	Windows	CVE-2018-8589	Microsoft released an update program for vulnerabilities of Windows. Among the vulnerabilities, Microsoft announced that an exploitation of CVE-2018-8589 had been identified [66]. According to Kaspersky, this vulnerability was used in a targeted attack aiming at the Middle East region in October [67].

Date	Product	Vulnerability number	Overview
December 5th	Adobe Flash Player	CVE-2018-15982	Adobe released an updated software version that fixes vulnerabilities that allow an arbitrary code execution and privilege escalation [68]. According to Gigamon, this vulnerability was used in a targeted attack aiming at a medical institution in Russia in November [69] (see Figure 7).
December 11th	Windows	CVE-2018-8611	Microsoft released an update program for vulnerabilities of Windows. Among the vulnerabilities, Microsoft announced that an exploitation of CVE-2018-8611 had been identified [70]. According to Kaspersky, multiple cyber attack groups including FruityArmor and SandCat had exploited this vulnerability [71].
December 19th	Internet Explorer	CVE-2018-8653	Microsoft had a non-regular release of a security update program. This program fixes a vulnerability that allows remote code execution in the Internet Explorer script engine. According to the discoverer, Google Threat Analysis Group, this vulnerability was used in a targeted attack [72].
December 21st	thinkPHP	-	A vulnerability was found in ThinkPHP, a PHP framework made in China, that allows remote code execution. Attack started on web servers of over 45,000 sites just after a security company (VulnSpy) published a PoC code [73].

Figure 5: SandboxEscaper publicizes a Windows vulnerability and PoC code by Twitter [61]

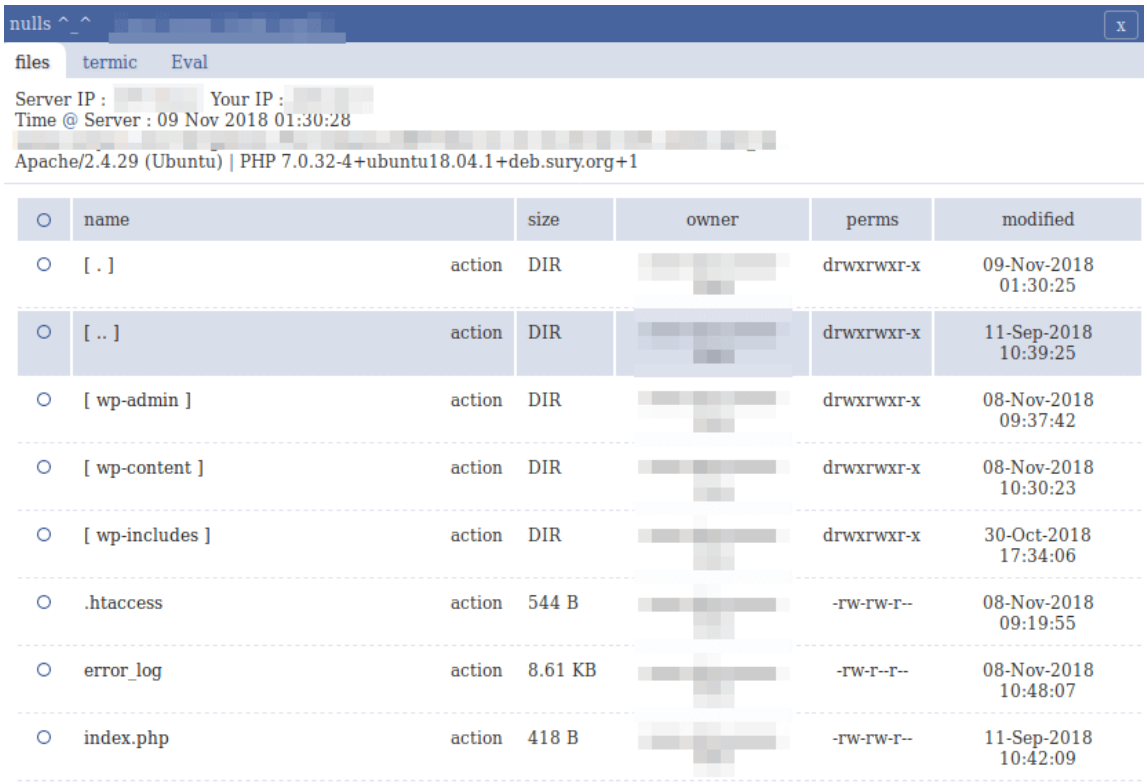


Figure 6 Screen showing a backdoor program installed in a compromised WordPress site [64]

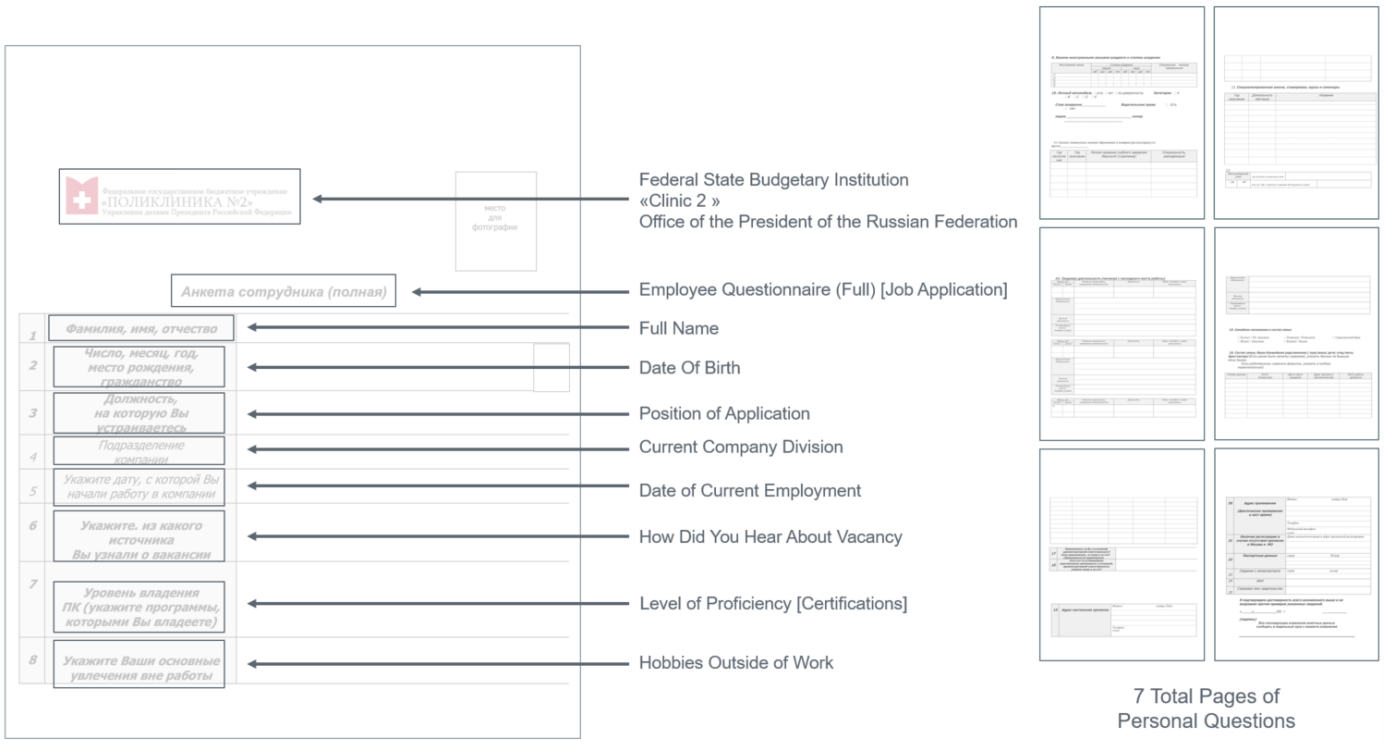


Figure 7 Malicious document disguised as an application form sent to a medical institution in Russia by a targeted attack email [69]

2.5.2. Botnet

In March and April 2018, two remote code execution vulnerabilities CVE-2018-7600 (Drupalgeddon) and CVE-2018-7602 were found consecutively in CMS software Drupal. On October 10th, IBM reported an attack that exploited these vulnerabilities to cause infection of botnet Shellbot [74]. Besides this one, there were other incidents that exploited vulnerabilities of IoT devices and routers to build a botnet as listed in the table below.

Table 11 Botnet incidents

Date	Product	Overview
October 25th	Hadoop	Radware reported that they found DemonBot, which exploited a vulnerability of remote code execution function of Hadoop YARN released in March 2018 to infect servers to build a botnet. In October, there were over one million attempts in a day that attacked the vulnerability [75] (see Figure 8).
November 1st	IoT devices, Linux servers, etc.	TrendMicro reported on a Perl-based botnet that attacked the vulnerability of IoT devices and Linux servers. An FTP server of a Japanese painting institution and a Dovecot email server of the Bangladesh government were exploited as C&C servers of the botnet [76].
November 7th	BroadCom routers, etc.	Qihoo 360 reported that a botnet consisting of over 100 thousand routers (see Figure 9) was delivering spam emails that infect computers with malware. The targets of the botnet were routers that had the UPnP function of BroadCom enabled [77].

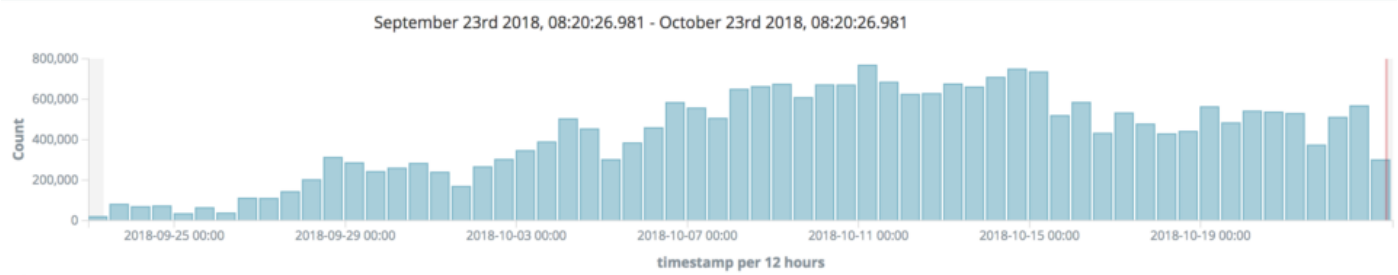


Figure 8 Number of access attempts from botnet DemonBot [75]

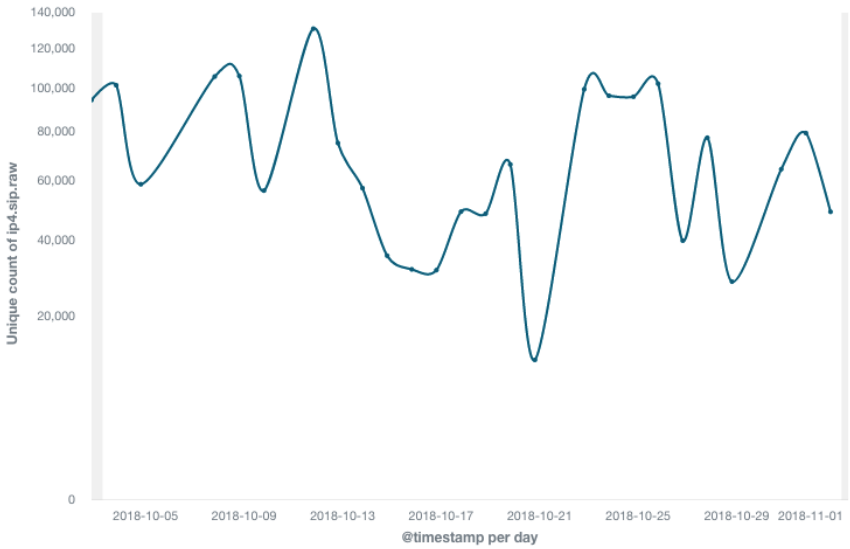


Figure 9 Number of routers that constitute the botnet [77]

2.5.3. Other attacks

Table 12 Other incidents of attacks that exploit vulnerabilities

Date	Product	Vulnerability number	Overview
November 6th	Kibana	CVE-2018-17246	A vulnerability was found that allowed insertion of files in Kibana, the frontend of Elasticsearch. An attacker could exploit this vulnerability to upload and execute any JavaScript file. The discoverer, CyberArk, publicized the vulnerability details and a PoC code on November 21st [78].
November 12th	Internet Explorer	CVE-2016-0189 CVE-2018-8373 CVE-2018-8174	Qihoo 360 reported that it found an attack that exploited a vulnerability of the VBScript engine of IE. According to the analysis of Qihoo 360, the attacker is a cyber attack group, DarkHotel. DarkHotel reportedly is connected to North Korea [79].
November 15th	nginx	CVE-2018-16843 CVE-2018-16844 CVE-2018-16845	Antuit reported that it detected a sign of an attack that would exploit a vulnerability of nginx. An update program has been released, without which a server may suffer a DoS attack or information theft. Correspondence on this vulnerability had increased sharply in dark webs and hacker forms [80].
December 1st	-	-	A Twitter user named TheHackerGiraffe had non-legitimate access to over 50 thousand printers to print a spam message (see Figure 10) that called for subscribing of YouTube channel PewDiePie. There also appeared a spam vendor (see Figure 11) that exploited this non-legitimate access to these printers to print messages [81].
December 3	Kubernetes	CVE-2018-1002105	A serious privilege escalation vulnerability was found in a container management software, Kubernetes. Gravitational publicized a PoC code on December 5th [82]. A researcher posted a demo video of the PoC on December 9th [83].

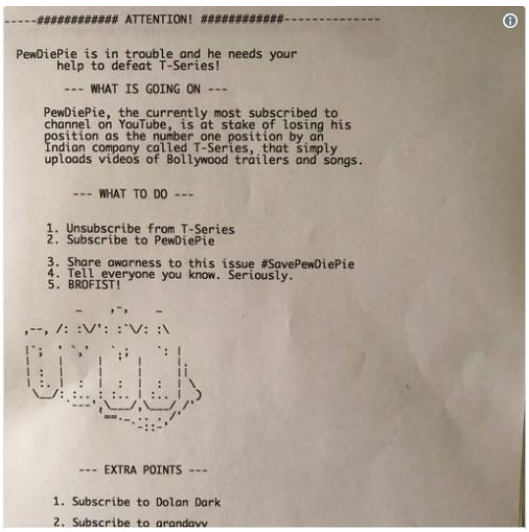


Figure 10 Spam message that calls for subscribing of YouTube channel PewDiePie [81]

Figure 11 Spam vendor declaring that it prints messages on printers

2.6. Malware

2.6.1. Ransomware

According to a report of Sophos, that aims at certain targets, are replacing conventional random targeting ones. There are also cases of interactive ransomware manually controlled by the attacker, and the damage of each incident is on the increase [84].

Table 13 Ransomware incidents

Date	Overview
October 25th	MalwareHunterTeam found that FilesLocker was offered as a new type of ransomware, RaaS (Ransomware as a Service). RaaS employs an affiliate scheme in which the vendor of this ransomware takes 60% from the earned ransom. There are Chinese and English versions [85].
November 25th	A medical institution in Ohio of the United States was infected with ransomware [86].
November 29th	The first cable car in Moscow was infected with ransomware on the next day of the opening, resulting in the suspension of cable car operation. Operation resumed on December 1st [87].
December 5th	Over 100 thousand computers were infected with ransomware in China. A malicious code was embedded in a development tool named EasyLanguage, so that programs developed by the tool were infected with the ransomware. The ransomware encrypted files and requested a ransom of 110 RMB (1,700 JPY) using WeChat, and stole credentials of online services (see Figure 12). The ransomware communicated with a C&C server using SNS service Douban. On December 6th, the China government arrested the person under the suspicion of making this ransomware [88].

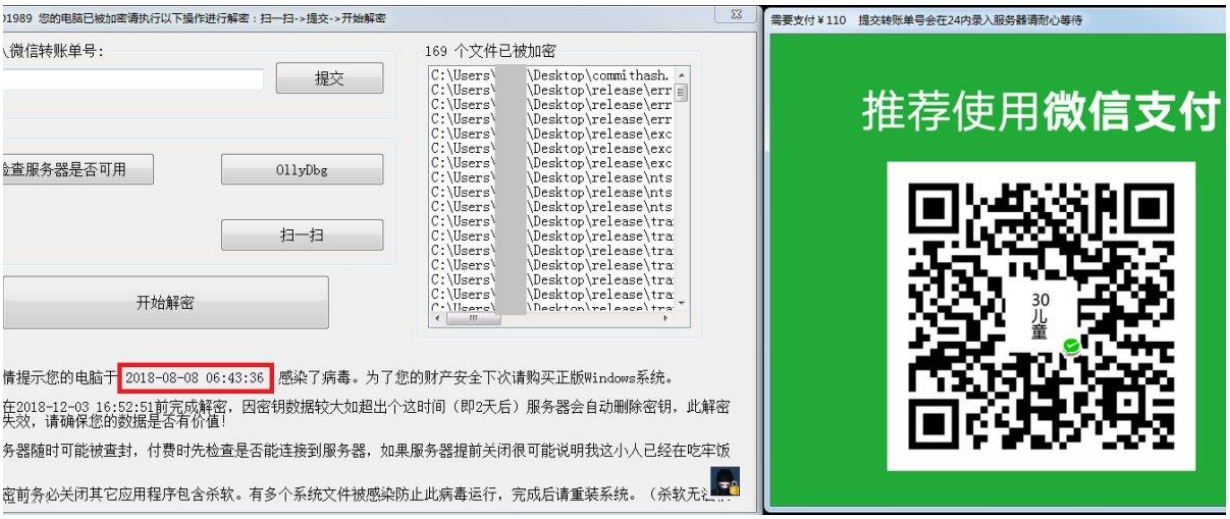


Figure 12 Ransomware screen requesting ransom [88]

2.6.2. Malware targeting Critical infrastructure

If a critical infrastructure such as electricity, gas, and water is stopped by a cyber attack, it will affect civilian life and corporate activities leading to danger of life and economic loss.

ESET reported that they found that the codes of malware Industroyer and NotPetya were similar (see Figure 13) on October 11 [89]. Cyber crime group TeleBots (BlackEnergy) engaged with these two cases of malware. Industroyer was used in an attack of a Ukraine power facility in 2016 to cause a power failure. Also, NotPetya prevailed in Ukraine in 2017 to cause damage to the government and financial institutions.

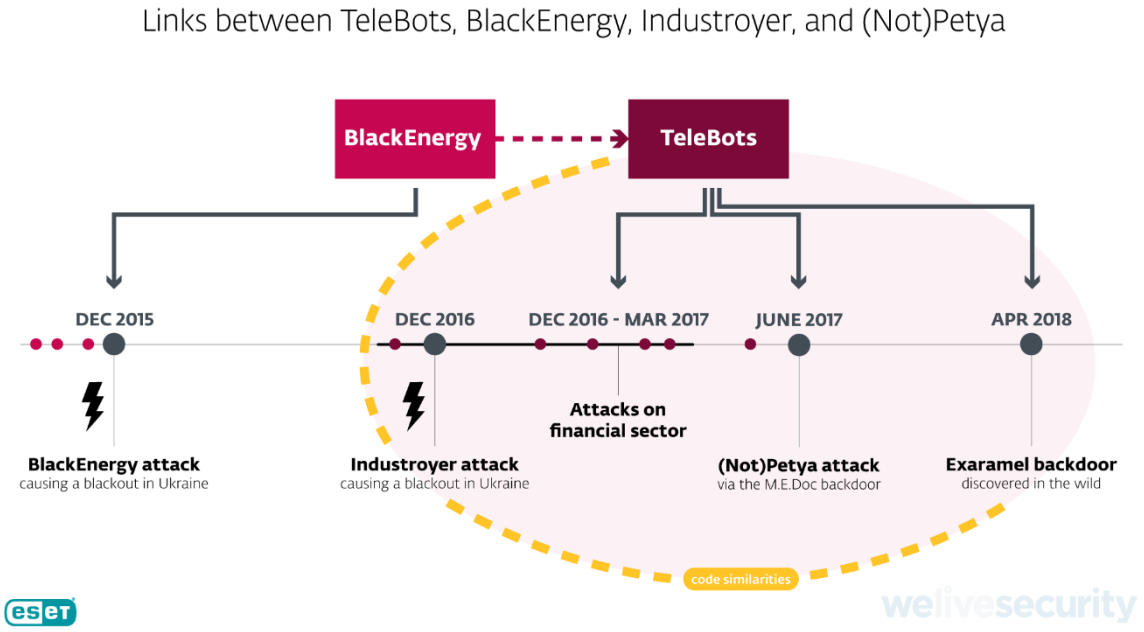


Figure 13 Relationship between malware Industroyer and NotPetya [89]

Table 14 Example of attacks on critical infrastructures

Date	Overview
October 15th	ONWASA, a waterworks bureau of North Carolina, the United States, was infected with malware Emotet. The bureau was force to rebuild the database to restore the service [90].
October 19th	Kaspersky reported an attack that exploited DanderSpritz and FuzzBunch—cyber attack tools said to have leaked from NSA. The attack infected 50 servers of Windows 2003/2008 in Russia, Iran, and Egypt. The targets were nuclear power station, telecommunication, IT, and R&D companies [91].
October 31st	A TV station of Israel broadcast that an infrastructure and the strategic network of Iran were attacked by malware similar to Stuxnet. Stuxnet is the malware used in the attack on a nuclear fuel facility of Iran in 2010 [92].
November 27th	Cisco reported a malware attack targeting sites related to the governments of Lebanon and UAE. The malware communicated with a C&C server using DNS queries and directed the victim to a malware distribution site using DNS redirect [93].

2.6.3. Malware targeting financial institutions and services

On October 2, US-CERT posted the result of analysis on FASTCash, which is the activity of a cyber attack group, HIDDEN COBRA, to unlawfully withdraw cash from ATMs. The US government relates HIDDEN COBRA with the North Korea government [94]. On October 3, FireEye posted a report on a cyber attack group, APT38. According to the report, the group stole over $1.1 billion from over 16 financial institutions of 13 countries from 2014. It is said that APT38 is connected with the North Korea government, so this cyber attack may become more intense when the North Korea government has difficulty in getting foreign currencies [95].

Table 15 Example attacks on financial institutions

Date	Overview
October 2nd	CheckPoint reported that banking malware DanaBot extended its scope of targets to include financial institutions of the United States. DanaBot is malware that steals credentials of online banking, and has been targeting Europe and Australia [96].
October 9th	Cylance reported that Banking trojan Panda Banker was extending its activity targeting the United States, Canada, and Japan. This trojan attempts to steal credit card information, personal information, cryptocurrency wallet information, and so forth [97].
November 7th	Banking trojan TrickBot now also collects information in Windows RAC[3], which stores software installation records and OS errors. The developer of this trojan is unknown. It could be used for phishing email attacks, for example [98].
November 16th	Group-IB reported phishing email attacks by cyber attack groups, MoneyTaker and Silence, on financial institutions in Russia. The phishing email disguised as an email from the central bank of Russia and had an attachment file that infects the computer when opened [99].
November 20th	Trend Micro found and reported an incident in which a cyber attack group, Lazarus, implanted a backdoor at a financial institution of Latin America [100].
November 22nd	Kaspersky reported mobile malware "Rotexy", which has the features of both banking trojans and ransomware. This malware eavesdrops SMS messages and disables devices to request a ransom. There were over 70 thousand attacks targeting mainly users in Russia [101].

[3] Reliability Analysis Component

Date	Overview
December 6th	Kaspersky reported a cyber attack on a bank of East Europe. The attacker entered the LAN of the bank using a netbook, Raspberry Pi, and Bash Bunny[4] to install a remote operation tool [102].
December 11th	ESET reported an Android Trojan that stole money from PayPal accounts. The Android Trojan horse passed two-factor authentication by exploiting the accessibility function of Android [103].
December 11th	A cyber crime group, Cobalt, has created a malicious Office document that installs a backdoor using the new version of an attacking tool, ThredKit. Cobalt excels at entering networks of financial institutions [104].
December 19th	Menlo Security reported an email attack targeting financial institutions of the United States and the United Kingdom. Executing the attachment file of the email infects the computer with a remote operation tool [105].

2.6.4. Other malware

Table 16 Examples of incidents of other malware

Date	Overview
October 11th	Cisco reported that it found a new type of Android Trojan horse that enabled dynamic changes of codes. This malware infects computers by disguised as Google Play Market and has functions such as inserting a plug-in from a remote location and compiling and deploying a new .NET source code [106] (See Figure 14).
October 11th	SANS reported that it found an attack that exploited a vulnerability (CVE-2017-11882) of the formula editor of Microsoft Office. This attack attaches a malicious document to an email to infect a computer with Trojan Razy [107].
October 24th	TrendMicro reported an attack that caused infection with malware by an email that was disguised as the postal service of Brazil. The characteristics of this attack were the used of Windows official programs wmic and certutil [108].
November 19th	A researcher of ESET found that false applications that were disguised as a drive simulator application were posted at Google Play. There were 13 such false applications and they were downloaded over 560 thousand times in total [109].
November 27th	Yoroi reported a spam email attack targeting Italy with a malicious PowerShell script. The script collects the information and screenshots of infected machines [110].
November 27th	Trend Micro reported a worm that infected computers via removable media. The worm is file-less type malware complied with the Autoit[5] language. It works as a keylogger or a DDoS tool [111].
November 28th	Forcepoint reported AutoCAD-based malware that targeted the industry field. The malware was written in the Lisp language and was used for industrial espionage. Infection was found in China, India, Turkey, and UAE [112].
December 11th	Trend Micro found a new type of exploit kit, Novidade, which targeted homes and SOHO routers. Novidade changes the DNS setting of a router using a CSRF vulnerability to direct the users in the domain of the router to a malicious site [113].

[4] Device that looks like a USB memory stick with which the user can execute programs on the connected computer.
[5] Programming language for Windows. Its main use is automatic operation of GUI. A compiled program can run on a machine without the Autoit runtime.

Figure 14 Malware that is disguised as Google Play Market (left) [106]

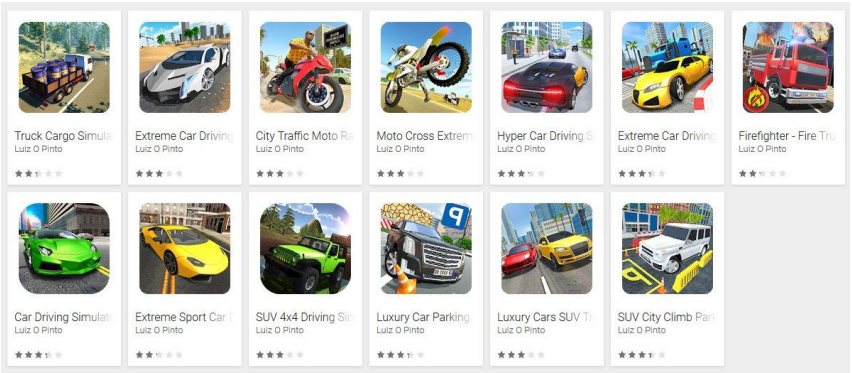
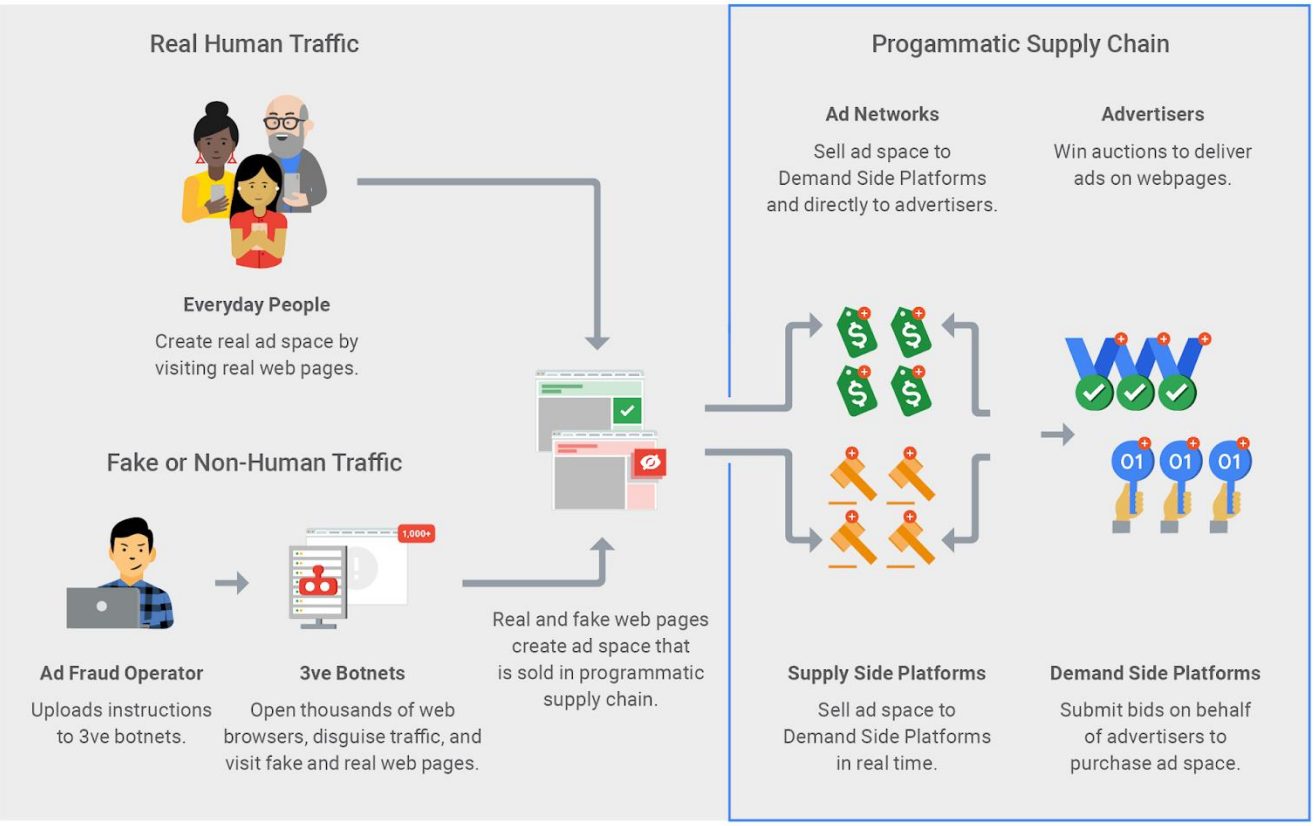


Figure 15 Android application that is disguised as a drive simulator [109]

2.6.5. Countermeasures against malware

The US Department of Justice announced that 3ve (pronounced "Eve") stopped its fraud advertisement botnet due to the arrest of members and the seizure of its domain [114]. Exploitation through 3ve includes unlawful earning of advertising revenues, malware infection, and BGP hijack. Damage by advertisement fraud is estimated $29 million [115] (see **Figure 16**).



An overview of the broader 3ve operation

Figure 16 Behavior of botnet 3ve [115]

Table 17 Cases of malware countermeasures

Date	Overview
October 16th	A Czech intelligence agency announced that it closed a server that Hezbollah[6] used to distribute malware. Hezbollah used malware to steal information from mobile devices of targets [116].
October 25th	ESET publicized a decrypting tool for a ransomware, GandCrab, for people suffering from Syria's civil war. The tool was made using the decryption key disclosed by the writer of GandCrab.
November 8th	The US cyber army (USCYBERCOM) provided malware samples at a malware analysis site, VirusTotal. The first provided sample was LoJack, which is often used by Fancy Bear[7].
December 5th	Blackhat Europe announced a new malware analysis service called SNDBOX. It is a free service of static and dynamic analysis based on machine learning [117].

[6] Shia terrorist organization based in Lebanon.
[7] A group suspected of a connection with the government of Russia. Also called as APT 28 or Sofacy.

2.7. IoT

There are increasing IT devices such as smart speakers and cameras that are always connected the Internet. Thus, there are increasing incidents related to IT devices. These devices may have unauthorized access if they have the following security defects:

- Firmware has vulnerability. Vulnerability is caused by the manufacturer not providing bug fixes or users not applying bug fixes.
- A weak password is used for access to the management screen of the device.
- An unnecessary service is running.

IT devices to be managed have increased, so people tend to forget some of them as devices to be managed or apply bug fixes to, resulting in the increase of incidents.

Table 18 Incidents of IoT attacks

Date	Overview
October 9th	SEC Consult reported that it found a serious vulnerability in a security camera manufactured by Hangzhou Xiongmai Technology of China. The report lists vulnerabilities including a weak administrator password, plaintext communication, and vulnerability in firmware update. The reporter estimates that approximately 9 million devices of the company are running in the world [118].
October 30th	CyberX published a report of a past 12-month research of threats on industrial control systems and IoT devices of 850 companies. Among the researched networks, 69% used plaintext passwords, 40% had direct communication with the Internet, and 57% were not adequately protected by antivirus software [119].

2.8. Security measures of governments, public institutions, and businesses

Table 19 Cases of security measures

Date	Overview
October 22th	The Financial Services Agency, Japan had "Cyber Security Training for the Entire Financial Industry" to raise the cyber incident competencies of small and mid-sized financial institutions. Cryptocurrency trading operators and FX operators also participated in the training in view of recent industry trends [120].
November 2nd	There was a report on NIST that it had a plan of using Watson of IBM to calculate CVSS scores. CVSS scores are calculated based on the complexity of attacks and the magnitude of risks. Waston is expected to provide faster score calculation with machine learning [121].
December 12th	IPA publicized "Twenty Best Practices for Safe Website Operation Management" (see Figure 17) in response to the increase of incidents such as data breach and web page falsification caused by the exploitation of website vulnerabilities and inadequate operation management [122].

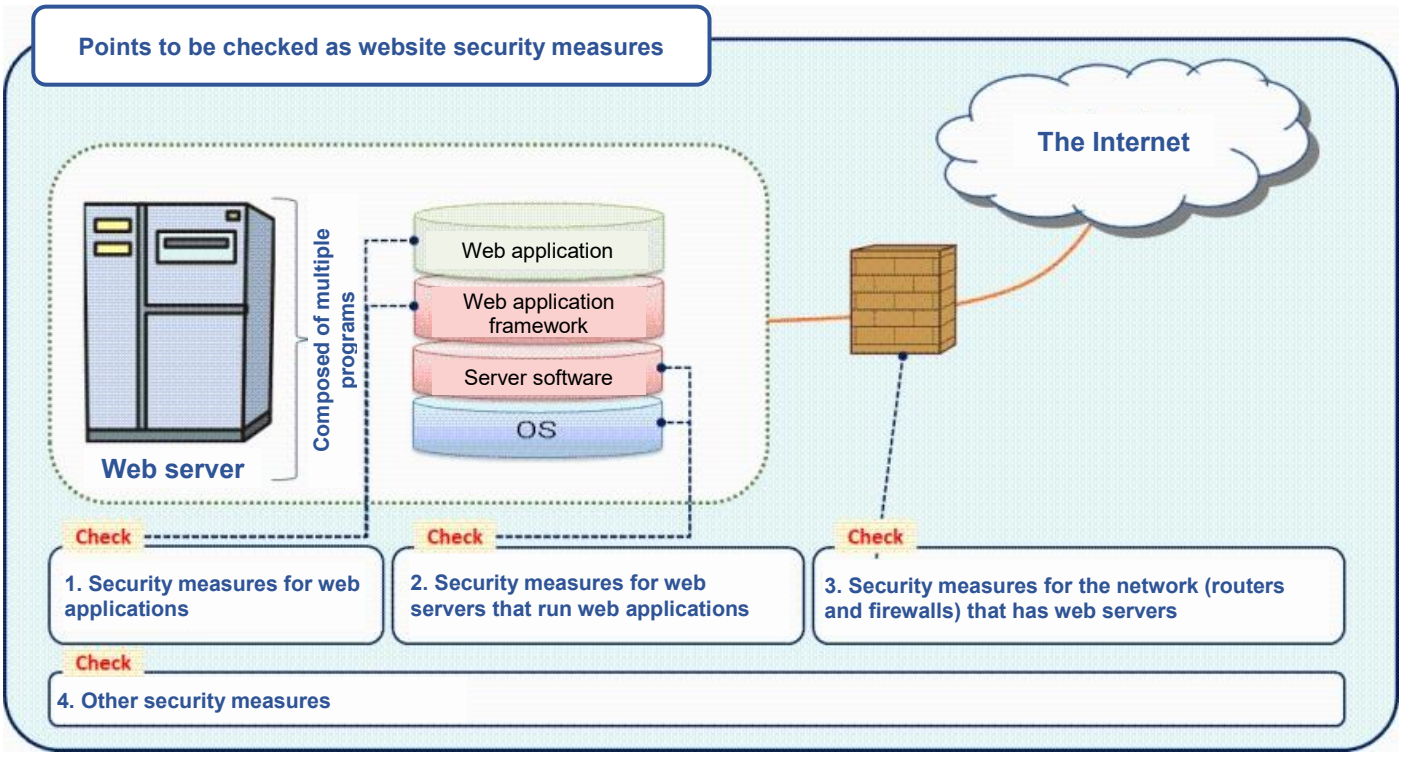


Figure 17 Points to be checked as website security measures [122]

3. Forecast on the 4th quarter of 2018 and thereafter

Attackers have had a hard time in profiting from unlawful mining due to the drop of cryptocurrency market prices. Attackers also seek return on investment, so they will turn resources that they have used for unlawful cryptocurrency earning to other unlawful means of earning money. NTTDATA-CERT forecasts that the following attacks will increase that use credentials unlawfully obtained by password list attacks[8] or other means:

- Business email compromise aiming at unlawful remittance
  The attacker sends emails disguised as a business partner or the accounting department using unlawfully obtained credentials to let the receiver remit money. Especially, there will be an increase in business email frauds exploiting the Office 365 service, of which corporate use is increasing.
- Blackmail requesting money
  The attacker unlawfully logs in to a computer of a company employee or a server using unlawfully obtained credentials to steal email attachments or documents in an online storage. The attacker earns money by blackmailing the company saying that it will leak the stolen information.
- Unlawful purchase
  The attacker logs in to an online shopping site disguised as a different person using unlawfully obtained credentials to purchase and resell goods or services that sell well. You should take it into account that there are certain number of employees who use online shopping sites using company email addresses.

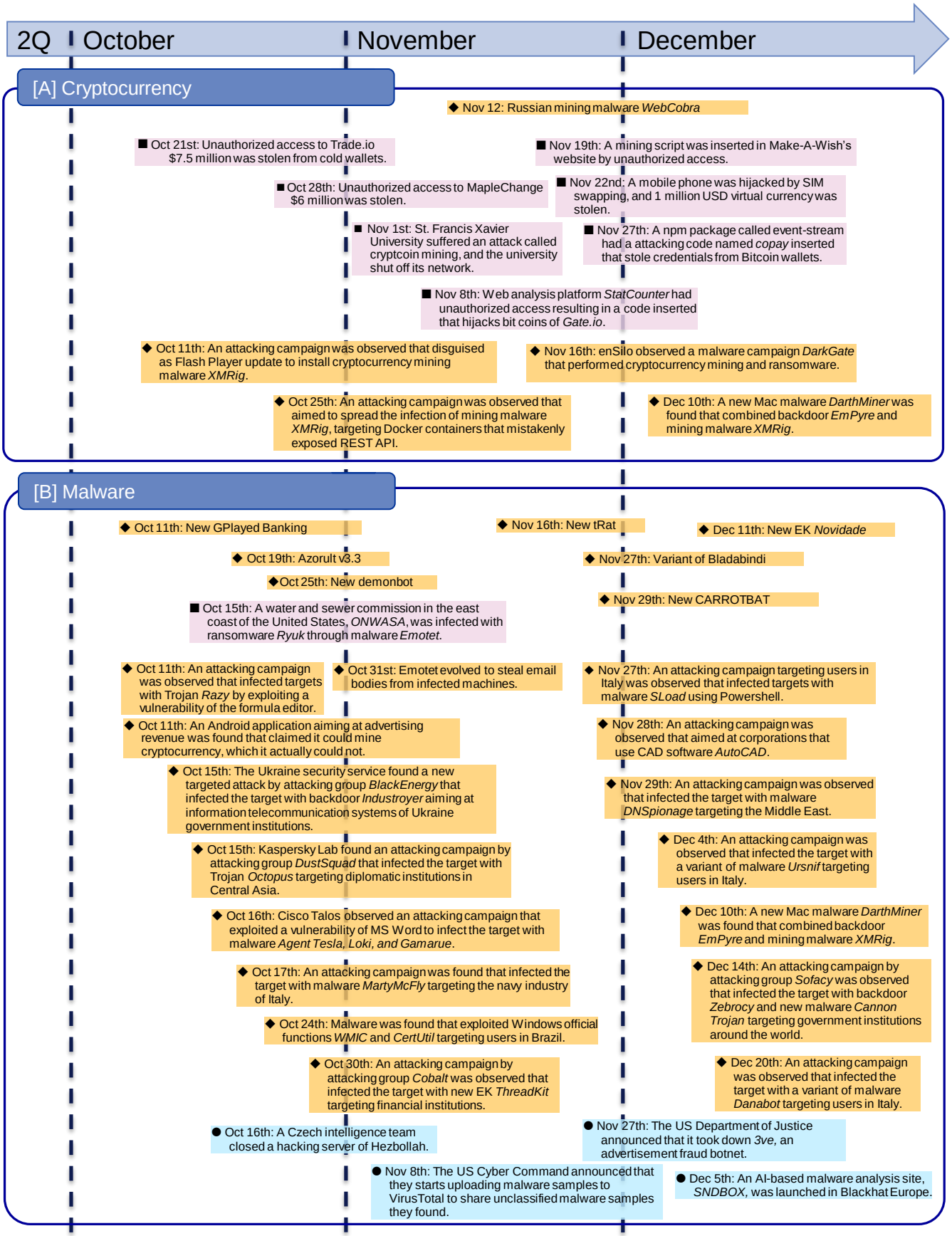
Corporations can prevent such attacks to mitigate damage by prohibiting the reuse of passwords among employees and employing stronger multi-factor or risk-based authentication.

[8] Attempts of unauthorized login to web services using the combination of user names and passwords that leaked to the Internet.

4. Timeline of 3rd quarter of 2018

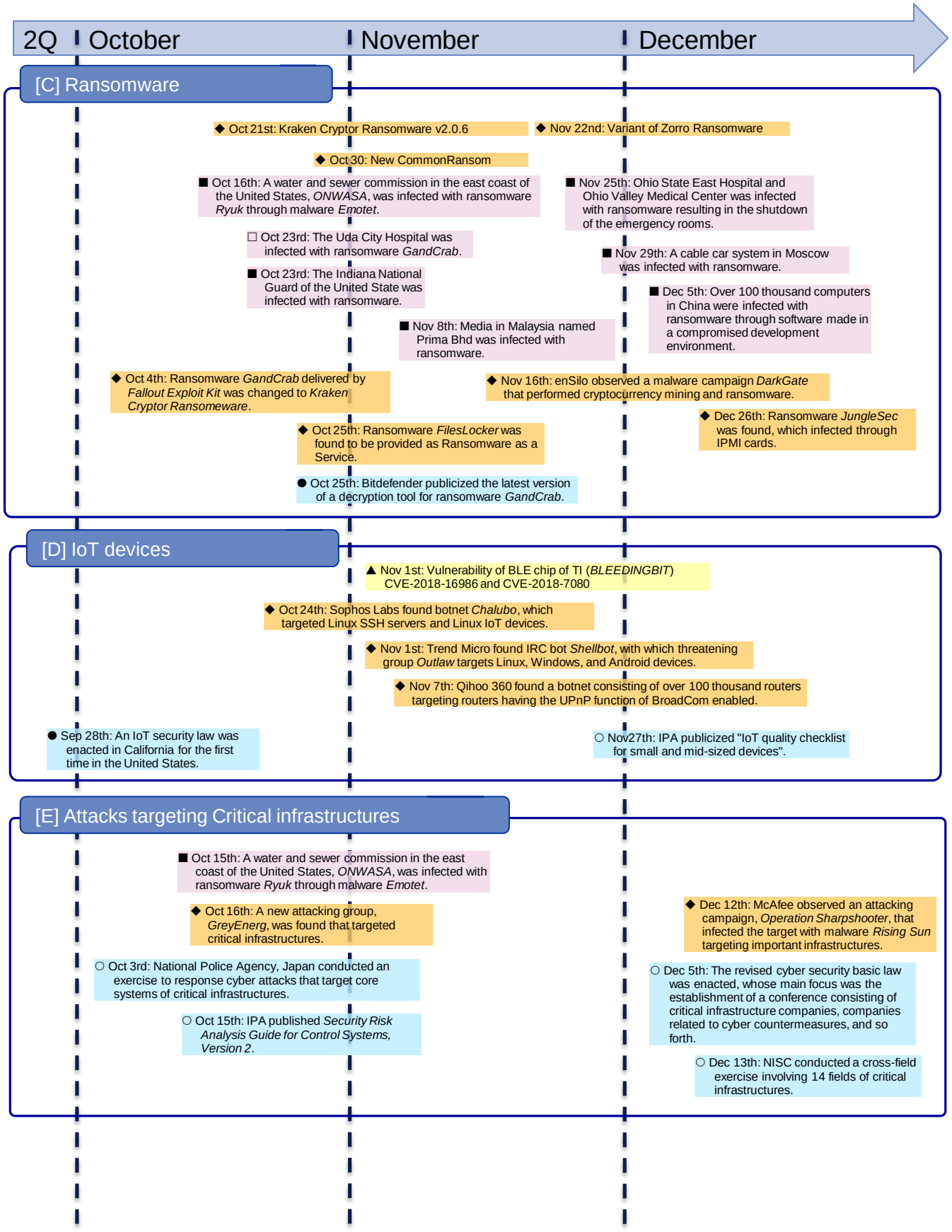
* Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○: Domestic ▲■◆●: Global/Overseas | △▲: Vulnerability □■: Incident | ◇◆: Threat ○●: Measure



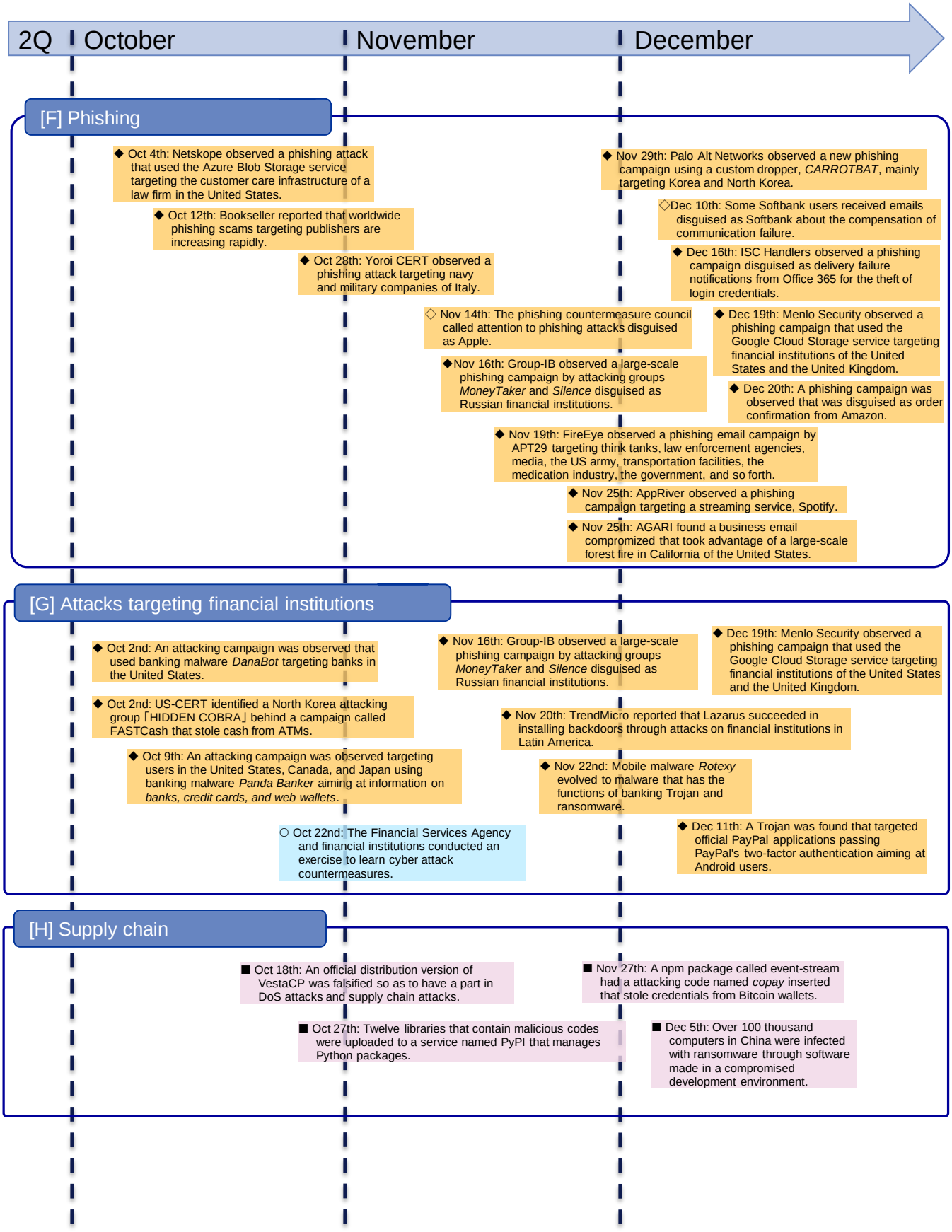
* Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○: Domestic ▲■◆●: Global/Overseas | △▲: Vulnerability □■: Incident | ◇◆: Threat ○●: Measure



* 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

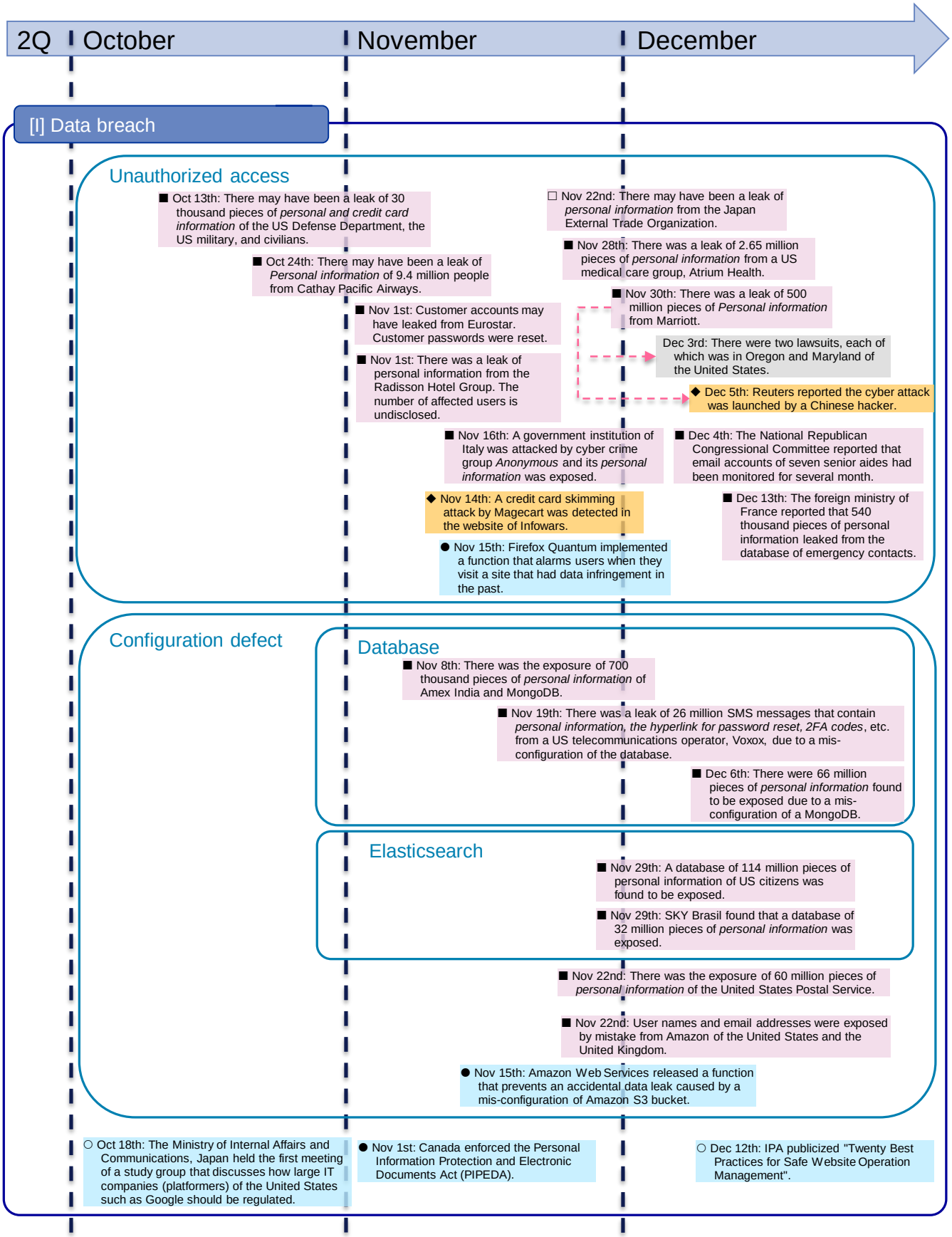


* Some of the dates on the timeline are dates of article issuance rather than dates of incident occurrence.

△□◇○: Domestic
▲■◆●: Global/Overseas

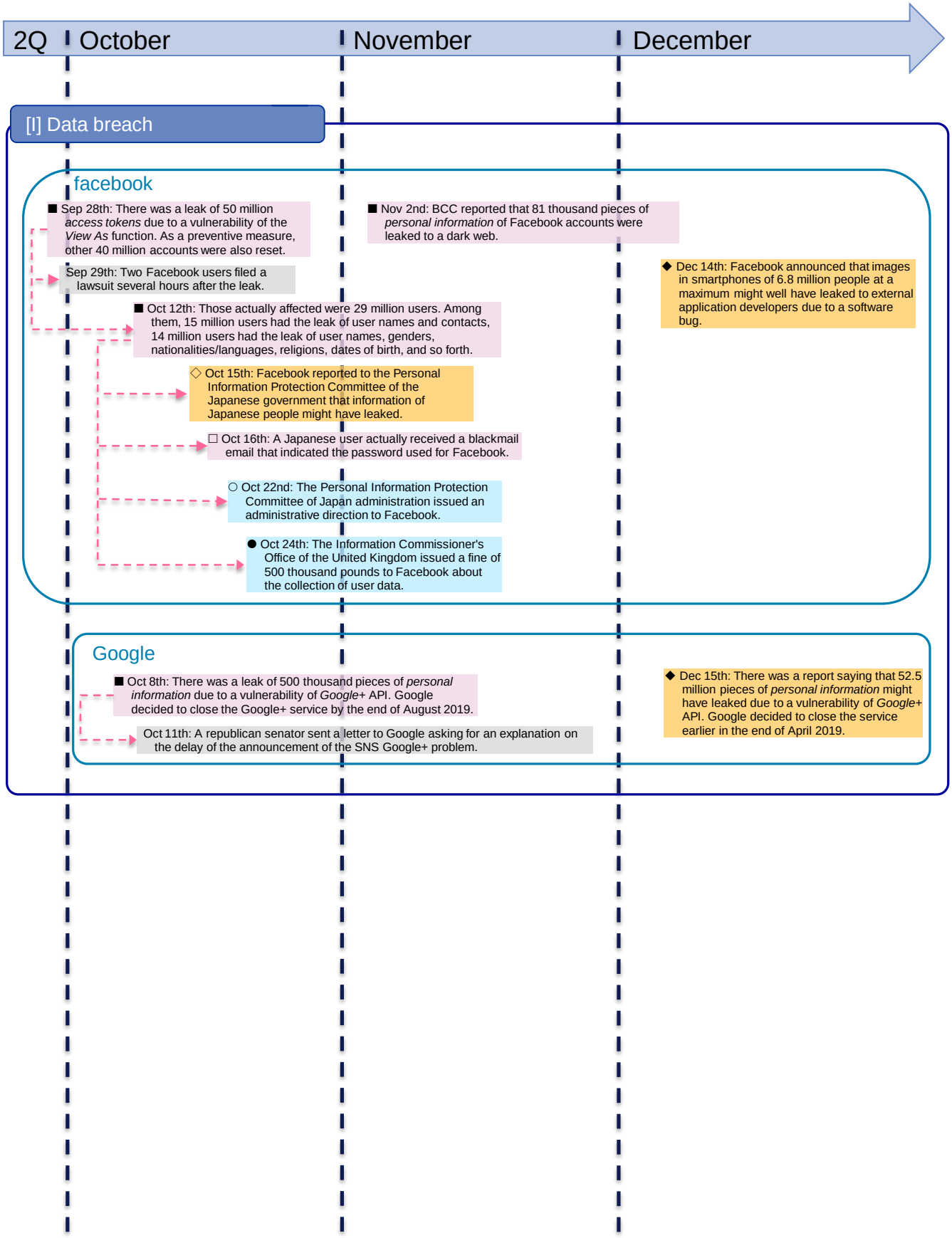
△▲: Vulnerability
□■: Incident

◇◆: Threat
○●: Measure



* 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



5. References

[1] 日本経済新聞社, "1400 万人の重要情報盗み見される フェイスブック," 13 10 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO36460990T11C18A0MM0000/.

[2] BBC Russian Service, "Private messages from 81,000 hacked Facebook accounts for sale," 2 11 2018. [Online]. Available: https://www.bbc.com/news/technology-46065796.

[3] 日本経済新聞, "FB、スマホ内の写真が流出の恐れ 最大 680 万人影響も," 15 12 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO38989240V11C18A2000000/.

[4] 個人情報保護委員会, "個人情報の保護に関する法律に基づく指導について," 22 10 2018. [Online]. Available: https://www.ppc.go.jp/news/press/2018/20181022/.

[5] CNET, "Facebook hit with $645,000 fine in UK over Cambridge Analytica scandal," [Online]. Available: https://www.cnet.com/news/uk-information-commissioners-office-hits-facebook-with-645000-fine/.

[6] Facebook, "Security Update," 28 9 2018. [Online]. Available: https://newsroom.fb.com/news/2018/09/security-update/.

[7] BLEEPING COMPUTER, "Google+ Shutting Down After Bug Leaks Info of 500k Accounts," 8 10 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/google-shutting-down-after-bug-leaks-info-of-500k-accounts/.

[8] ZDNet, "New Magecart hack detected at Shopper Approved," 9 10 2018. [Online]. Available: https://www.zdnet.com/article/new-magecart-hack-detected-at-shopper-approved/.

[9] AP NEWS, "Pentagon reveals cyber breach of travel records," 13 10 2018. [Online]. Available: https://www.apnews.com/7f6f4db35b0041bdbc5467848225e67d.

[10] CATHAY PACIFIC, "Data security event," 24 10 2018. [Online]. Available: https://infosecurity.cathaypacific.com/en_HK.html.

[11] Security Affairs, "New attack by Anonymous Italy: personal data from ministries and police have been released online," 6 11 2018. [Online]. Available: https://securityaffairs.co/wordpress/77717/hacktivism/anonymous-italy-attacks.html.

[12] Security Affairs, "689,272 plaintext records of Amex India customers exposed online," 8 11 2018. [Online]. Available: https://securityaffairs.co/wordpress/77815/data-breach/amex-india-data-leak.html.

[13] BLEEPING COMPUTER, "Infowars Store Affected by Magecart Credit Card Stealing Hack," 14 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/infowars-store-affected-by-magecart-credit-card-stealing-hack/.

[14] BLEEPING COMPUTER, "US Postal Service Exposes Data of 60 Million Users for Over a Year," 22 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/us-postal-service-exposes-data-of-60-million-users-for-over-a-year/.

[15] BLEEPING COMPUTER, "Marriott Data Breach Affects 500 Million Starwood Guests," 30 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/marriott-data-breach-affects-500-million-starwood-guests/.

[16] Help Net Security, "Health websites routinely share your activity with 57 third-parties," 9 10 2018. [Online]. Available: https://www.helpnetsecurity.com/2018/10/09/health-websites-privacy/.

[17] 産経新聞, "グーグルなどへの規制強化も 総務省研究会が初会合," 18 10 2018. [Online]. Available: https://www.sankei.com/economy/news/181018/ecn1810180016-n1.html.

[18] ZDNet, "Android news and kids apps contain the most third-party trackers," 18 10 2018. [Online]. Available: https://www.zdnet.com/article/android-news-and-kids-apps-contain-the-most-third-party-trackers/.

[19] CNET, "Location data from a gas station app sold for $9.50 per 1,000 people," 10 12 2018. [Online]. Available: https://www.cnet.com/news/location-data-from-a-gas-station-app-sold-for-9-50-per-1000-people/.

[20] IPA 独立行政法人 情報処理推進機構, "宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に～ 不審アプリのインストールに加えて、フィッシングにも注意！ ～," [Online]. Available: https://www.ipa.go.jp/security/anshin/mgdayori20181129.html.

[21] 日本サイバー犯罪対策センター事務局, "不正送金等の犯罪被害につながるメールに注意," 7 11 2016. [Online]. Available: https://www.jc3.or.jp/topics/virusmail.html.

[22] 佐川急便株式会社, "佐川急便を装った迷惑メールにご注意ください," 10 10 2018. [Online]. Available: http://www2.sagawa-exp.co.jp/whatsnew/detail/721/.

[23] 時事通信社, "佐川急便かたるメールに注意," [Online]. Available: https://www.jiji.com/jc/p?id=20180817082809-0027960591.

[24] Netskope, "Phishing in the public cloud: You've been served," 3 10 2018. [Online]. Available: https://www.netskope.com/blog/phishing-in-the-public-cloud.

[25] Bleeping Computer, "Phishing Attacks Distributed Through CloudFlare's IPFS Gateway," 4 10 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/phishing-attacks-distributed-through-cloudflares-ipfs-gateway/.

[26] Menlo Security, "A "JAR" Full of Problems for Financial Services Companies," 19 12 2018. [Online]. Available: https://www.menlosecurity.com/blog/a-jar-full-of-problems-for-financial-services-companies.

[27] PhishLabs, "49 Percent of Phishing Sites Now Use HTTPS," 6 12 2018. [Online]. Available: https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.

[28] ZDNet, "Trade.io loses $7.5Mil worth of cryptocurrency in mysterious cold wallet hack," 22 10 2018. [Online]. Available: https://www.zdnet.com/article/trade-io-loses-7-5mil-worth-of-cryptocurrency-in-mysterious-cold-wallet-hack/.

[29] "MapleChange Crypto Exchange Hacked For Bitcoin (BTC)," 30 10 2018. [Online]. Available: https://ethereumworldnews.com/maplechange-crypto-exchange-hacked-for-913-bitcoin-btc-exit-scam-likely/.

[30] 株式会社 Doctor Web Pacific, "Doctor Web による報告:オンラインスキャマーにより 24,000 ドルを超える被害、被害者数は 10,000 人超え," 19 10 2018. [Online]. Available: https://news.drweb.co.jp/show/?lng=ja&i=12886&c=5.

[31] ZDNet, "Hackers breach StatCounter to hijack Bitcoin transactions on Gate.io exchange," 6 11 2018. [Online]. Available: https://www.zdnet.com/article/hackers-breach-statcounter-to-hijack-bitcoin-transactions-on-gate-io-exchange/.

[32] Ars Technica, "Widely used open source software contained bitcoin-stealing backdoor," 27 11 2018. [Online]. Available: https://arstechnica.com/information-technology/2018/11/hacker-backdoors-widely-used-open-source-software-to-steal-bitcoin/.

[33] NEW YORK POST, "Man hacked into Silicon Valley execs' phones to steal cryptocurrency: cops," 20 11 2018. [Online]. Available: https://nypost.com/2018/11/20/man-hacked-into-silicon-valley-execs-phones-to-steal-cryptocurrency-cops/.

[34] ZDNet, "SIM-swapping 21-year-old scores $1 million by hijacking a phone," 22 11 2018. [Online]. Available: https://www.zdnet.com/article/sim-swapping-21-year-old-scores-1-million-by-hijacking-a-phone/.

[35] 日経新聞社, "仮想通貨狙いウイルス作成疑い、家裁送致 名古屋地検," 28 11 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO38288260Y8A121C1CN8000/.

[36] McAfee Labs, "McAfee Labs Threats Report December 2018," 18 12 2018. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.

[37] Bleeping Computer, "CoinMiners Use New Tricks to Impersonate Adobe Flash Installers," 11 10 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/coinminers-use-new-tricks-to-impersonate-adobe-flash-installers/.

[38] NICTER, "継続する 5555/TCP ポート宛攻撃通信と ADB が有効化された脆弱な Android エミュレータについて," 22 10 2018. [Online]. Available: https://blog.nicter.jp/2018/10/android-5555/.

[39] JVN, "JVN#60702986," 24 10 2018. [Online]. Available: https://jvn.jp/jp/JVN60702986/.

[40] TREND MICRO, "Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware," 25 10 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/misconfigured-container-abused-to-deliver-cryptocurrency-mining-malware/.

[41] ST. FRANCIS XAVIER UNIVERSITY, "STFX SYSTEMS UPDATE," 4 11 2018. [Online]. Available: https://www.stfx.ca/about/news/stfx-systems-update-0.

[42] McAfee, "WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency," 12 11 2018. [Online]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/.

[43] Trustwave, "Hacker's Wish Come True After Infecting Visitors of Make-A-Wish Website With Cryptojacking," 19 11 2018. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hackers-wish-come-true-after-infecting-visitors-of-make-a-wish-website-with-cryptojacking/.

[44] Bloomberg Businessweek, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," 4 10 2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2.

[45] Bloomberg Businessweek, "The Big Hack: Statements From Amazon, Apple, Supermicro, and the Chinese Government," 4 10 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond.

[46] Amazon, "Setting the Record Straight on Bloomberg BusinessWeek's Erroneous Article," 4 10 2018. [Online]. Available: https://aws.amazon.com/jp/blogs/security/setting-the-record-straight-on-bloomberg-businessweeks-erroneous-article/.

[47] REUTERS, "中国による悪意のチップ埋め込み疑う根拠なし＝英政府機関," 8 10 2018. [Online]. Available: https://jp.reuters.com/article/china-cyber-britain-idJPKCN1MI0B7.

[48] SCRIBD, "Letter October 8th Version," 8 10 2018. [Online]. Available: https://ja.scribd.com/document/390401381/Letter-October-8th-Version.

[49] Bloomberg, "Senate Panel Seeks FBI Briefing on Super Micro Hacking Report," 2 11 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-11-01/senate-panel-seeks-fbi-briefing-on-super-micro-hacking-report.

[50] Super Micro, "Supermicro Refutes Claims in Bloomberg Article," 11 12 2018. [Online]. Available: https://www.supermicro.com/newsroom/pressreleases/2018/press181004_Bloomberg.cfm.

[51] THE WALL STREET JOURNAL, "Washington Asks Allies to Drop Huawei," 23 11 2018. [Online]. Available: https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105?tesla=y.

[52] REUTERS, "New Zealand rejects Huawei's first 5G bid citing national security risk," 28 11 2018. [Online]. Available: https://www.reuters.com/article/us-spark-nz-huawei-tech/new-zealand-government-agency-rejects-sparks-plan-to-use-huawei-5g-equipment-idUSKCN1NX08U?feedType=RSS&feedName=technologyNews.

[53] engadget, "ファーウェイ CFO がカナダで逮捕。米国からの要請、対イラン制裁に違反した疑い," 6 12 2018. [Online]. Available: https://japanese.engadget.com/2018/12/05/cfo/.

[54] REUTERS, "英ＢＴ、５Ｇで華為製品使用せず　３Ｇ・４Ｇからも排除," 6 12 2018. [Online]. Available: https://jp.reuters.com/article/bt-group-huawei-tech-idJPKBN1O42V1.

[55] RUTERS, "ドイツ、ファーウェイを政府調達から排除せず　５Ｇ整備巡り," 8 12 2018. [Online]. Available: https://jp.reuters.com/article/germany-telecoms-idJPKBN1O628P.

[56] 日本経済新聞, "機密漏洩防止へ調達指針　政府、ファーウェイ念頭," 10 12 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO38728050Q8A211C1MM0000/.

[57] CNN.co.jp, "ファーウェイ製品の採用、仏独通信大手が方針見直し," 15 12 2018. [Online]. Available: https://www.cnn.co.jp/tech/35130180.html.

[58] Microsoft, "CVE-2018-8453 | Win32k の特権の昇格の脆弱性," 9 10 2018. [Online]. Available: https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2018-8453.

[59] Kaspersky, "Zero-day exploit (CVE-2018-8453) used in targeted attacks," 10 10 2018. [Online]. Available: https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/.

[60] Bleeping Computer, "New Windows Zero-Day Bug Helps Delete Any File, Exploit Available," 23 10 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-windows-zero-day-bug-helps-delete-any-file-exploit-available/.

[61] ZDNet, "Microsoft Windows zero-day disclosed on Twitter, again," 23 10 2018. [Online]. Available: https://www.zdnet.com/article/microsoft-windows-zero-day-disclosed-on-twitter-again/.

[62] Cisco, "Cisco Adaptive Security Appliance Software and Cisco Firepower Threat Defense Software Denial of Service Vulnerability," 31 10 2018. [Online]. Available: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181031-asaftd-sip-dos.

[63] S. Zelenyuk, "VirtualBox E1000 Guest-to-Host Escape," 7 11 2018. [Online]. Available: https://github.com/MorteNoir1/virtualbox_e1000_0day.

[64] Wordfence, "Trends Emerging Following Vulnerability In WP GDPR Compliance Plugin," 9 11 2018. [Online]. Available: https://www.wordfence.com/blog/2018/11/trends-following-vulnerability-in-wp-gdpr-compliance-plugin/.

[65] WP GDPR Compliance Plugin, "WP GDPR Compliance 1.4.3 Security Release," 7 11 2018. [Online]. Available: https://www.wpgdprc.com/wp-gdpr-compliance-1-4-3-security-release/.

[66] Microsoft, "CVE-2018-8589 | Windows Win32k の特権の昇格の脆弱性," 13 11 2018. [Online]. Available: https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2018-8589.

[67] Kaspersky, "A new exploit for zero-day vulnerability CVE-2018-8589," 14 11 2018. [Online]. Available: https://securelist.com/a-new-exploit-for-zero-day-vulnerability-cve-2018-8589/88845/.

[68] Adobe, "Security updates available for Flash Player | APSB18-42," 5 12 2018. [Online]. Available: https://helpx.adobe.com/security/products/flash-player/apsb18-42.html.

[69] Gigamon, "Adobe Flash Zero-Day Exploited In the Wild," 5 12 2018. [Online]. Available: https://atr-blog.gigamon.com/2018/12/05/adobe-flash-zero-day-exploited-in-the-wild/.

[70] Microsoft, "CVE-2018-8611 | Windows カーネルの特権の昇格の脆弱性," 11 12 2018. [Online]. Available: https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2018-8611.

[71] Kaspersky, "Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611)," 12 12 2018. [Online]. Available: https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/.

[72] Bleeping Computer, "Microsoft Releases Out-of-Band Security Update for Internet Explorer RCE Zero-Day," 19 12 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-releases-out-of-band-security-update-for-internet-explorer-rce-zero-day/.

[73] ZDNet, "Chinese websites have been under attack for a week via a new PHP framework bug," 21 12 2018. [Online]. Available: https://www.zdnet.com/article/chinese-websites-have-been-under-attack-for-a-week-via-a-new-php-framework-bug/.

[74] IBM, "Threat Actors Prey on Drupalgeddon Vulnerability to Mass-Compromise Websites and Underlying Servers," 10 10 2018. [Online]. Available: https://securityintelligence.com/threat-actors-prey-on-drupalgeddon-vulnerability-to-mass-compromise-websites-and-underlying-servers/.

[75] Radware, "New DemonBot Discovered," 25 10 2018. [Online]. Available: https://blog.radware.com/security/2018/10/new-demonbot-discovered/.

[76] TrendMicro, "Perl-Based Shellbot Looks to Target Organizations via C&C," 1 11 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/perl-based-shellbot-looks-to-target-organizations-via-cc/.

[77] Qihoo 360, "BCMPUPnP_Hunter: A 100k Botnet Turns Home Routers to Email Spammers," 7 11 2018. [Online]. Available: https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/.

[78] CyberArk, "A Local File Inclusion in Kibana allows attackers to run local JavaScript file," 21 11 2018. [Online]. Available: https://www.cyberark.com/threat-research-blog/execute-this-i-know-you-have-it/.

[79] Qihoo 360, "A Missed 0day ? - Reveal another Cyber Arsenal of APT-C-06," 12 11 2018. [Online]. Available: http://blogs.360.cn/post/VBScript_vul_EN.html.

[80] 時事通信, "Nginx の脆弱性を悪用する攻撃準備中か、ダークウェブの観察で判明," 15 11 2018. [Online]. Available: https://this.kiji.is/435938239837946977?c=220450040231249399.

[81] Forbes, "A Hacker Forced 50,000 Printers To Spread PewDiePie Propaganda -- And The Problem Is Much Bigger Than You Know," 3 12 2018. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2018/12/03/a-hacker-forced-50000-printers-to-spread-pewdiepie-propagandaand-the-problem-is-much-bigger-than-you-know/.

[82] Gravitational, "gravitational/cve-2018-1002105," 5 12 2018. [Online]. Available: https://github.com/gravitational/cve-2018-1002105.

[83] Twistlock, "Demystifying Kubernetes CVE-2018-1002105 (and a dead simple exploit)," 9 12 2018. [Online]. Available: https://www.twistlock.com/labs-blog/demystifying-kubernetes-cve-2018-1002105-dead-simple-exploit/.

[84] Sophos, "ソフォスの「2019 年版脅威レポート」: 被害者から数百万ドルを搾取する、特定ユーザーを狙った標的型攻撃の台頭が明らかに," 22 11 2018. [Online]. Available: https://www.sophos.com/ja-jp/press-office/press-releases/2018/11/sophoslabs-2019-threat-report.aspx.

[85] Bleeping Computer, "New FilesLocker Ransomware Offered as a Ransomware as a Service," 25 10 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-fileslocker-ransomware-offered-as-a-ransomware-as-a-service/.

[86] The Times Leader, "Hospitals: Patient information safe in EORH, OVMC computer attack," 25 11 2018. [Online]. Available: http://www.timesleaderonline.com/news/local-news/2018/11/hospitals-patient-information-safe-in-eorh-ovmc-computer-attack/.

[87] Bleeping Computer, "Moscow's New Cable Car System Infected with Ransomware the Day After it Opens," 30 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/moscows-new-cable-car-system-infected-with-ransomware-the-day-after-it-opens/.

[88] Bleeping Computer, "Ransomware Infects 100K PCs in China, Demands WeChat Payment," 5 12 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/.

[89] ESET, "New TeleBots backdoor: First evidence linking Industroyer to NotPetya," 11 10 2018. [Online]. Available: https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/.

[90] ONWASA, "Cyber-criminals target critical utility in hurricane-ravaged area," 15 10 2018. [Online]. Available: https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A.

[91] Kaspersky, "DarkPulsar," 19 10 2018. [Online]. Available: https://securelist.com/darkpulsar/88199/.

[92] The Times of Israel, "TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet," 31 10 2018. [Online]. Available: https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/.

[93] Cisco, "DNSpionage Campaign Targets Middle East," 27 11 2018. [Online]. Available: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html.

[94] US-CERT, "HIDDEN COBRA – FASTCash Campaign," 2 10 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-275A.

[95] FireEye, "北朝鮮国家の支援を受ける 新たな脅威グループ「APT38」の詳細を発表," 3 10 2018. [Online]. Available: https://www.fireeye.com/blog/jp-threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html.

[96] Proofpoint, "DanaBot Gains Popularity and Targets US Organizations in Large Campaigns," 2 10 2018. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns.

[97] Cylance, "Threat Spotlight: Panda Banker Trojan Targets the US, Canada and Japan," 9 10 2018. [Online]. Available: https://threatvector.cylance.com/en_us/home/threat-spotlight-panda-banker-trojan-targets-the-us-canada-and-japan.html.

[98] Bleeping Computer, "TrickBot Banking Trojan Starts Stealing Windows Problem History," 17 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-starts-stealing-windows-problem-history/.

[99] Group-IB, "Two hacker groups attacked Russian banks purporting to be the Central Bank of Russia," 16 11 2018. [Online]. Available: https://www.group-ib.com/media/cbrf-double-attack/.

[100] Trend Micro, "Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America," 20 11 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/.

[101] Kaspersky, "The Rotexy mobile Trojan – banker and ransomware," 22 11 2018. [Online]. Available: https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/.

[102] Kaspersky, "DarkVishnya: Banks attacked through direct connection to local network," 6 12 2018. [Online]. Available: https://securelist.com/darkvishnya/89169/.

[103] ESET, "Android Trojan steals money from PayPal accounts even with 2FA on," 11 12 2018. [Online]. Available: https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/.

[104] Bleeping Computer, "Cobalt Bank Robbers Use New ThreadKit Malicious Doc Builder," 11 12 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/cobalt-bank-robbers-use-new-threadkit-malicious-doc-builder/.

[105] Menlo Security, "A "JAR" Full of Problems for Financial Services Companies," 19 12 2018. [Online]. Available: https://www.menlosecurity.com/blog/a-jar-full-of-problems-for-financial-services-companies.

[106] Cisco, "GPlayed Trojan - .Net playing with Google Market," 11 10 2018. [Online]. Available: https://blog.talosintelligence.com/2018/10/gplayedtrojan.html.

[107] SANS, "New Campaign Using Old Equation Editor Vulnerability," 11 10 2018. [Online]. Available: https://isc.sans.edu/forums/diary/New+Campaign+Using+Old+Equation+Editor+Vulnerability/24196/.

[108] TrendMicro, "Malware Targeting Brazil Uses Legitimate Windows Components WMI and CertUtil as Part of its Routine," , 24 10 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/malware-targeting-brazil-uses-legitimate-windows-components-wmi-and-certutil-as-part-of-its-routine/.

[109] Bleeping Computer, "Fake Apps in Google Play Get over Half a Million Installs," 19 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-apps-in-google-play-get-over-half-a-million-installs/.

[110] Yoroi, "The SLoad Powershell Threat is Expanding to Italy," 27 11 2018. [Online]. Available: https://blog.yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/.

[111] Trend Micro, "AutoIt-Compiled Worm Affecting Removable Media Delivers Fileless Version of BLADABINDI/njRAT Backdoor," 27 11 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/.

[112] Forcepoint, "AutoCAD Malware - Computer Aided Theft," 28 11 2018. [Online]. Available: https://www.forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft.

[113] Trend Micro, "New Exploit Kit “Novidade” Found Targeting Home and SOHO Routers," 11 12 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/.

[114] Department of Justice, "Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud," 27 11 2018. [Online]. Available: https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing.

[115] Bleeping Computer, "3ve Ad Fraud Botnet with Billions of Daily Ad Requests Shut Down," 27 11 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/3ve-ad-fraud-botnet-with-billions-of-daily-ad-requests-shut-down/.

[116] ZDNet, "Czech intelligence service shuts down Hezbollah hacking operation," 16 10 2018. [Online]. Available: https://www.zdnet.com/article/czech-intelligence-service-shuts-down-hezbollah-hacking-operation/.

[117] Bleeping Computer, "SNDBOX - an AI Powered Malware Analysis Site is Launched," 5 12 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/sndbox-an-ai-powered-malware-analysis-site-is-launched/.

[118] SEC Consult, "REMOTE CODE EXECUTION VIA XMEYE P2P CLOUD IN XIONGMAI IP CAMERAS, NVRS AND DVRS," 9 10 2018. [Online]. Available: https://sec-consult.com/en/blog/advisories/vulnerabilities-xiongmai-ip-cameras-nvrs-dvrs-cve-2018-17915-cve-2018-17917-cve-2018-17919/.

[119] CyberX, "2019 GLOBAL ICS & IIOT RISK REPORT," 30 10 2018. [Online]. Available: https://cyberx-labs.com/resources/risk-report-2019.

[120] 金融庁, "「金融業界横断的なサイバーセキュリティ演習," 19 10 2018. [Online]. Available: https://www.fsa.go.jp/news/30/sonota/20181019/20181019-cyber.html.

[121] Nextgov, "NIST Teams Up with IBM's Watson to Rate How Dangerous Computer Bugs Are," 2 11 2018. [Online]. Available: https://www.nextgov.com/cybersecurity/2018/11/nist-teams-ibms-watson-rate-how-dangerous-computer-bugs-are/152545/.

[122] IPA, "安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～," 12 12 2018. [Online]. Available: https://www.ipa.go.jp/security/vuln/websitecheck.html.

[123] Yoroi, "Cyber-Espionage Campaign Targeting the Naval Industry ("MartyMcFly")," 17 10 2018. [Online]. Available: https://blog.yoroi.company/research/cyber-espionage-campaign-targeting-the-naval-industry-martymcfly/.

[124] Kryptos Logic, "Emotet Awakens With New Campaign of Mass Email Exfiltration," 31 10 2018. [Online]. Available: https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html.

[125] Yoroi, "Dissecting the latest Ursnif DHL-Themed Campaign," 4 12 2018. [Online]. Available: https://blog.yoroi.company/research/dissecting-the-latest-ursnif-dhl-themed-campaign/.

[126] ABC30 News, "Girl Scouts' personal information affected by recent data breach," 26 10 2018. [Online]. Available: https://abc30.com/4561129/.

[127] MSE News, "Eurostar customers told to reset passwords after attempted hack," 31 10 2018. [Online]. Available: https://www.moneysavingexpert.com/news/2018/10/eurostar-customers-told-to-reset-passwords-after-attempted-hack/.

[128] ZDNet, "Radisson Hotel Group suffers data breach, customer info leaked," 2018, 1 11. [Online]. Available: https://www.zdnet.com/article/radisson-hotel-group-chain-suffers-data-breach/.

[129] The New York Times, "FIFA, Hacked Again, Braces for New Revelations," 30 10 2018. [Online]. Available: https://www.nytimes.com/2018/10/30/sports/soccer/fifa-uefa-hack.html.

[130] BBC, "HSBC bank confirms US data breach," [Online]. Available: https://www.bbc.com/news/technology-46117963.

[131] ITmedia, "Amazon ユーザーの氏名やメールアドレス、手違いで公開," 22 11 2018. [Online]. Available: http://www.itmedia.co.jp/news/articles/1811/22/news060.html.

[132] 警察庁, "仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について," 12 3 2018. [Online]. Available: https://www.npa.go.jp/cyberpolice/important/2018/201803121.html.

February 13th, 2019

NTT DATA Corporation
NTTDATA-CERT,
Information Security Office, Security Engineering Department

nttdata-cert@kits.nttdata.co.jp