NTT DATA
Trusted Global Innovator

# NTTDATA-CERT Global Security Quarterly Report: April - June 2018

August 13th, 2018 (Revised November 20th, 2018)
NTT DATA Corporation

# Table of Contents

Executive Summary

I. Hot Topic

II. Forecast

III. Timeline

References

# Executive Summary

The General Data Protection Regulation (GDPR) was enforced on May 25. Companies providing services for EU residents are required to pay more attention to handling of personal information. Cyber attacks targeting cryptocurrencies for monetary purpose are actively carried out. The number of ransomware attacks is decreasing, but medical institutions and critical systems are targeted for ransom money. Basic preventive measures against malware, such as fixing vulnerability of software, installing and updating anti-virus software and backing up data, are still important.

**(1) Domestic and overseas trends to protect personal information**

- On March 17, it was revealed by a newspaper that Cambridge Analytica, a UK consulting firm for elections, had exploited personal information obtained from Facebook for its business without permission. Facebook announced that up to 87 million users were involved. SNS users should use SNS considering risks that information posted on the SNS or provided for the SNS applications could be leaked or exploited.
- On June 14, information was leaked from a hotel booking service provider Fastbooking due to unauthorized access. Japanese hotels which outsourced the booking service to them were also involved, which drew attention as a GDPR case.

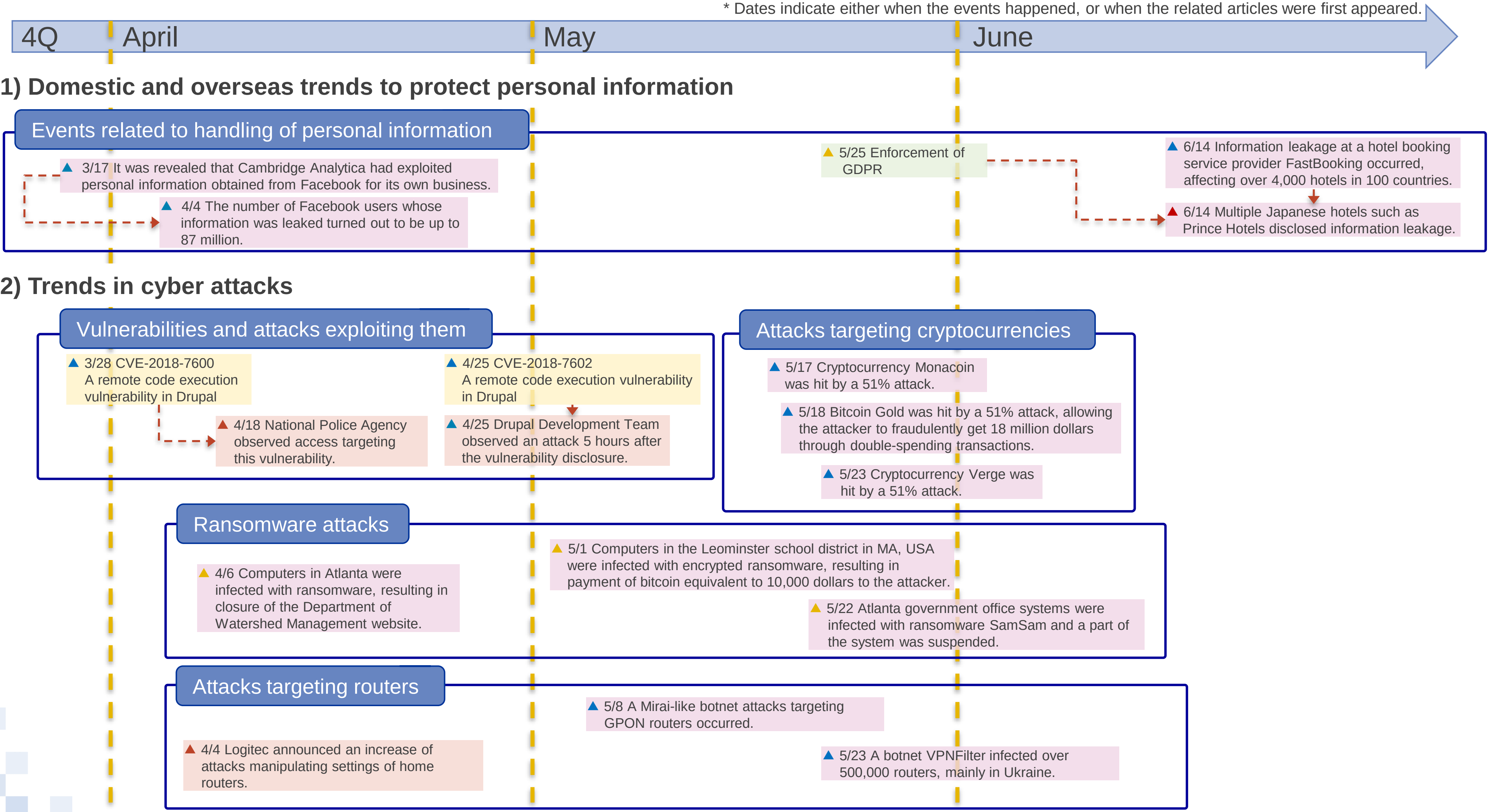
**(2) Trends in cyber attacks**

- The Verge, Bitcoin Gold and Monacoin cryptocurrencies were hit by 51% attacks, causing double-spending transactions at the exchanges of the above cryptocurrencies. Until then, a real threat of 51% attacks was said to be low, but the above case revealed necessity of measures in the exchanges against 51% attacks.
- Multiple cases were found where large-scale botnets were formed exploiting vulnerabilities and insecure configurations of routers. Venders requested their customers to update firmware, change the default password, and not to publish the management interface to the Internet.

# Executive Summary – Time line of related events –

▲: Globally common 🟨: Vulnerabilities 🟦: Countermeasures
▲: Specific regional 🟧: Threats 🟩: Governments
▲: Domestic in Japan 🟪: Cyber attacks/incidents

* Dates indicate either when the events happened, or when the related articles were first appeared.



## (1) Domestic and overseas trends to protect personal information

### Events related to handling of personal information

▲ 3/17 It was revealed that Cambridge Analytica had exploited personal information obtained from Facebook for its own business.

▲ 4/4 The number of Facebook users whose information was leaked turned out to be up to 87 million.

▲ 5/25 Enforcement of GDPR

▲ 6/14 Information leakage at a hotel booking service provider FastBooking occurred, affecting over 4,000 hotels in 100 countries.

▲ 6/14 Multiple Japanese hotels such as Prince Hotels disclosed information leakage.

## (2) Trends in cyber attacks

### Vulnerabilities and attacks exploiting them

▲ 3/28 CVE-2018-7600 A remote code execution vulnerability in Drupal

▲ 4/18 National Police Agency observed access targeting this vulnerability.

▲ 4/25 CVE-2018-7602 A remote code execution vulnerability in Drupal

▲ 4/25 Drupal Development Team observed an attack 5 hours after the vulnerability disclosure.

### Attacks targeting cryptocurrencies

▲ 5/17 Cryptocurrency Monacoin was hit by a 51% attack.

▲ 5/18 Bitcoin Gold was hit by a 51% attack, allowing the attacker to fraudulently get 18 million dollars through double-spending transactions.

▲ 5/23 Cryptocurrency Verge was hit by a 51% attack.

### Ransomware attacks

▲ 4/6 Computers in Atlanta were infected with ransomware, resulting in closure of the Department of Watershed Management website.

▲ 5/1 Computers in the Leominster school district in MA, USA were infected with encrypted ransomware, resulting in payment of bitcoin equivalent to 10,000 dollars to the attacker.

▲ 5/22 Atlanta government office systems were infected with ransomware SamSam and a part of the system was suspended.

### Attacks targeting routers

▲ 4/4 Logitec announced an increase of attacks manipulating settings of home routers.

▲ 5/8 A Mirai-like botnet attacks targeting GPON routers occurred.

▲ 5/23 A botnet VPNFilter infected over 500,000 routers, mainly in Ukraine.

# I. Hot Topic (1/11)
(1) Events related to handling of personal information

## (1) Events related to handling of personal information

### (1-1) Enforcement of GDPR and its effects

On May 25, the General Data Protection Regulation (GDPR) was enforced. The GDPR is a framework, formulated by the European Parliament and the European Council, to protect personal information. It is expected to have a great influence as it applies to not only all data managers and processors based in EU but also enterprises providing goods and services for EU. Especially, an influence on "WHOIS", which provides a service that allows users to obtain information on an owner of a domain or IP address through the Internet, attracted great attention. Currently, a method called "phased access" is adopted, and installation of a system to give access permission to the police department, brand proprietors and security personnel is underway.

### (1-2) GDPR-related phishing scam emails

On May 22, Avira called attention to GDPR-related phishing scam emails (*1-1). These scam emails pretend to be notifications requesting agreement on changes in the personal information policy or handling of personal information accompanied by the enforcement of the GDPR, asking users to enter their personal information in a webpage or infecting the computers with malware. The users must be careful as similar phishing scam emails pretending to be famous companies such as Apple, PayPal and Airbnb have been reported. The users must carefully handle emails related to the GDPR such as by not clicking links unnecessarily or checking whether any suspicious details are contained.

# I. Hot Topic (2/11)
## (1) Events related to handling of personal information

### (1-3) Case examples that could be violating the GDPR

Global companies, especially those providing services for EU residents, must pay more and more attention to information handling, both internally and at their subcontractors, etc., due to the enforcement of the GDPR.

- On May 25, an NGO noyb filed a case against four companies including Google and Facebook. It claimed that those companies forced new privacy policies on users, violating the GDPR (*1-2).
- On June 26, Prince Hotels announced that 124,963 cases of personal data had been leaked. This was caused by unauthorized access to the booking system servers for English, Korean and Chinese in Fastbooking, a booking service provider of Prince Hotels (*1-3).

### (1-4) Personal information handling in SNS

News related to Facebook’s personal information protection drew great public attention.

- On March 17, unauthorized sharing of data of 50 million people with Cambridge Analytica attracted public interest (*1-4).
- On April 4, unauthorized sharing of data with Cambridge Analytica was revealed to affect 87 million people (*1-5).
- On April 10 and 11, Facebook CEO Mark Zuckerberg was called at the US Congress because of some cases including unauthorized data use by Cambridge Analytica. Zuckerberg apologized for multiple issues, saying that he had not taken sufficient measures against the misuse and it had been his fault (*1-6).

When giving personal information to SNS and cloud services, care should be taken such as by reading terms of service carefully, avoiding provision of unnecessary information and setting the scope of information sharing properly. In addition, SNS users should use SNS considering risks such as leakage and unauthorized use of information posted on SNS and given to SNS applications.

# I. Hot Topic (3/11)
## (2) Attacks targeting routers

### (2) Attacks targeting routers

### (2-1) Attacks targeting routers for business use

- On April 5, Cisco Talos called attention to attacks exploiting a vulnerability of Cisco Smart Install Client, CVE-2018-0171 (*2-1). Over 168,000 routers all over the world, and over 10,000 routers in Japan were vulnerable (*2-2).

  The volume of traffic searching Cisco Smart Install Client had been increasing since November 2017 (see Figure 1) and further increased just after the vulnerability CVE-2018-0171 was announced in March. Attackers could easily find vulnerable routers using searching tools such as Shodan, which drastically increased attacks.

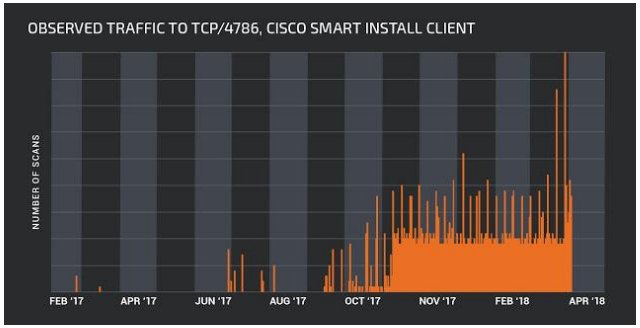


Figure 1: Traffic to Cisco Smart Install Client's port (Sourced from Cisco "Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client (*2-1)")

- On April 16, the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) in the US and the National Cyber Security Centre (NCSC) in the UK jointly released a warning on Russian Government cyber activities (*2-3). They stated that cyber attacks exploiting the vulnerability of Cisco Smart Install Client were carried out targeting government and private sector network devices.

# I. Hot Topic (4/11)
## (2) Attacks targeting routers

### (2-2) Attacks targeting routers for consumers

- Malware VPNFilter infected over 500,000 routers for consumers all over the world (*2-4). VPNFilter sets a three-step attack against routers for consumers.
- Infection by malware Roaming Mantis spread especially in the Asian region. Roaming Mantis tampers the DNS settings of routers and steals personal and credit card information such as by installing malware into or displaying a phishing website on Android terminals which have accessed to the Internet via the routers (*2-5). In Japan, routers for consumers made by computer accessory manufacturers such as Logitec and Buffalo suffered from the attacks (*2-6).

### (2-3) Countermeasures against these attacks

- The manufacturers informed that users should contact them immediately when an attack on their routers is suspected. Typical countermeasures against the attacks targeting routers include updating the firmware of the routers to the latest version, changing the default password of the management interface to a complex one and not disclosing the management interface to the Internet.
- Restarting routers infected with VPNFilter can delete malware infected at the second and the third steps. As malware infected at the fist step is installed in the non-volatile memory in the routers, they should be reset to the factory settings to delete the malware.
- On March 6, the Ministry of Internal Affairs and Communications submitted to the Congress a proposal to revise the act on the National Institute of Information and Communications Technology (NICT) (*2-7). This is to allow the NICT under the Ministry of Internal Affairs and Communications to investigate and identify vulnerable IoT devices and to call attention to the users.

Countermeasures taken by consumers themselves are limited. It is expected that security venders and network device manufacturers provide auto-update and that manufactures strengthen countermeasures satisfying the standards established by the government.

# I. Hot Topic (5/11)
## (3) Attacks targeting cryptocurrencies

### (3) Attacks targeting cryptocurrencies

**Classification of attacks**
Table 1 shows classification of attacks targeting cryptocurrencies by the transaction and the target. In the past reports, this classification was used to consolidate data by comparing it against attacks targeting traditional currencies. In this report, attacks are classified by the target.

**Table 1: Classification of attacking techniques targeting cryptocurrencies**

| Transaction of cryptocurrency | Target | Description and example of attacks |
|---|---|---|
| Parties involved in cryptocurrency transactions | Cryptocurrency service providers･･･(3-1) | Attacks targeting the wallet of cryptocurrency exchanges |
| | Cryptocurrency service users | Attacks stealing authentication information used to login to the cryptocurrency exchanges |
| Regardless of cryptocurrency transactions | PC owners･･･(3-2) | Infecting cryptocurrency miners. Drive-by mining, etc. |

### (3-1) Attack against cryptocurrency service providers

- On May 22, a transaction application Taylor was hacked, with cryptocurrency equivalent to 1.5 million dollars stolen (*3-1).
- On May 23, a cryptocurrency Verge was hit by a 51% attack, resulting in damage of 1 million dollars equivalent (*3-2).
- On June 10, ICO tokens equivalent to 40 million dollars were stolen from a Korean cryptocurrency exchange Coinrail (*3-3).
- On June 20, cryptocurrency equivalent to 31 million dollars was stolen from a Korean cryptocurrency exchange Bithumb (*3-4).

A 51% attack refers to an attack performing fraudulent transactions by controlling a majority of calculation necessary for cryptocurrency transactions. One of the countermeasures against the 51% attack at cryptocurrency exchanges is to increase the number of approvals confirmed at each transaction. This makes the transaction less affected by fraudulent operation of the blockchain even if a specific attacker accounts for the majority of calculation. The users can avoid all of the above attacks by moving their funds from the wallet in the exchange to their self-managed wallet after each transaction.

# I. Hot Topic (6/11)
## (3) Attacks targeting cryptocurrencies

### (3-2) Attacks targeting PC owners

- On June 16, a Chinese security company Qihoo 360 reported an epidemic of malware WinstarNssmMiner.
  This malware infected approx. 500,000 PCs within three days by cryptojacking (*) and mined cryptocurrency Monero equivalent to 28,000 dollars fraudulently (*3-5). One of the countermeasures against this is to use a web browser protected from the cryptojacking or a browser extension having a similar function.
  (*) Cryptojacking: a case where malicious third parties embed malicious codes in a website and execute the codes on PCs of the site visitors without permission to fraudulently mine cryptocurrencies
- Amazon Fire TV and Fire TV Stick were also infected with malware ADB.Miner, which infected Android devices and mined cryptocurrency Monero (*3-6). When such devices as Fire TV are infected with malware, users may notice some symptoms such as the video stopping immediately or not being able to play. Devices infected with malware should be reset to the factory settings to delete the malware.

Attackers are focusing their efforts on attacks such as the above to get cryptocurrencies fraudulently through PC owners because the attacks are more reliable than ransomware to make profits. General users who are not cryptocurrency exchanges or cryptocurrency users also need to be careful about infection of malware which mines cryptocurrency using CPU resources of PC.

# I. Hot Topic (7/11)
## (4) Ransomware attacks

### (4) Ransomware Satan now has a function for spreading infection

In the mid-April 2018, many attacks utilizing EternalBlue were observed. These attacks are assumed to be carried out by ransomware Satan (also known as DBGer) using EternalBlue (*4-1). Satan provides cloud services for various operations such as creating ransomware, collecting ransom money and providing an encoding tool for victims who have paid ransom money. These services are called RaaS (Ransomware as a Service).

The following functions for spreading infection were added to Satan.

- January 2017: Satan was discovered (*4-2).
- November 2017: Satan started to use EternalBlue to spread infection (*4-3).
- May 2018: Satan started to use vulnerabilities of JBoSS and Weblogic to spread infection (*4-4).
- June 2018: Satan changed its name to DBGer and started to use Mimikatz to spread infection (*4-5).

Compared to Cerber, one of the well-known RaaS, Satan differs in the following aspects:

- The share of ransom money paid to the cloud service provider is 30% in the case of Satan (*4-2) and 40% in the case of Cerber (*4-6).
- Satan has functions for spreading infection.
  Cerber has functions for avoiding detection and stealing cryptocurrencies (*4-7).

# (5) Attacks on supply chains

## (5) Attacks on supply chains

### (5-1) Attacks targeting software developers

- It was found out that a backdoor was embedded in the getcookies package registered in “Node Packaged Modules (npm)”, which manages JavaScript environment for servers, Node. js (*5-1).
- A backdoor stealing SSH authentication information was found out to be embedded in the Python module “SSH Decorator”. The developer reports that the module embedded with the backdoor was fraudulently uploaded on the distribution website (*5-2).
- GitHub accounts of Gentoo Linux were hacked, and malware for deleting files were installed (*5-3).

Some cases have been reported where developers’ accounts for software distribution websites were hacked. This requires countermeasures such as installing multi-factor authentication for software distribution websites.

### (5-2) Inserting malicious codes in image files

Malicious PowerShell scripts were embedded in skins (PNG file) for changing the appearance of avatars in a sandbox game Minecraft.
The fact that Minecraft: Java Edition users can upload customized skins onto the Minercraft website was misused (*5-4).
In this case, it is reported that downloading skins alone will not execute the code (*5-5).

Figure 2: Skins embedded with malicious scripts (Sourced from Avast “Minecraft players exposed to malicious code in modified ‘skins’ (*5-4)”)

# I. Hot Topic (9/11)
# (6) Policy not requiring periodic password changes

### (6-1) Opposition to periodic password changes

It was discovered by domestic and overseas researches that forcing periodic password changes increases risks instead because users tend to use a simple password or reuse a password. Introduction of multi-factor authentication and risk-based authentication is expected to accelerate in the future instead of the periodic password changes.

- December 2017: NIST stated in SP800-63B (Digital Identity Guidelines) that service providers should not request periodic password changes (*6-1).
- December 2017: NISC specified in its information security handbook that periodic password changes are not necessary (*6-2).
- March 2018: Ministry of Internal Affairs and Communications specified in the information security website for citizens that “periodic password changes are not necessary”.
- April 2018: JIPDEC, a PrivacyMark issuing agency, modified the examination standards for certification so that it does not require periodic password changes in using the Internet (*6-3).
- April 2018: Yahoo announced a policy that it would delete the statement for encouraging periodic password changes (*6-4).

Some services may request periodic password changes, but the users do not have to change their passwords unless there is a fact that their passwords have been stolen and the accounts have been hacked, or that their passwords have been leaked from the service providers.

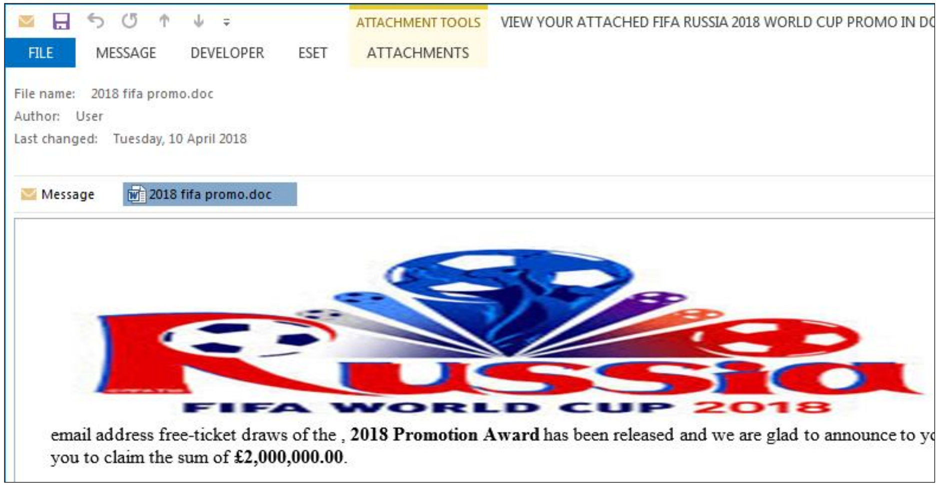
Sourced from the Ministry of Internal Affairs and Communications “For Safe Use of the Internet: Information Security Website for the Citizens”
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html

# I. Hot Topic (10/11)
## (7) Cyber attacks related to international events

### (7) Cyber attacks related to international events

### (7-1) 2018 FIFA World Cup Russia

- On June 4, fake messages of official jersey wins were spread in Whatsapp targeting Brazilian users (*7-1).
- On June 6, email scams of FIFA World Cup-related lottery wins were discovered (*7-2).
- On June 14, a person from a US intelligence agency stated that mobile devices of people travelling in Russia may be fraudulently accessed by the Russian government (*7-3).
- On July 6, the Ministry of Defense in Israel announced that an attack targeting soldiers of Israel to install Android spyware occurred. The spyware was disguised as a news flash app for World Cup game results (*7-4).



File name: 2018 fifa promo.doc
Author: User
Last changed: Tuesday, 10 April 2018

email address free-ticket draws of the , **2018 Promotion Award** has been released and we are glad to announce to yo
you to claim the sum of **£2,000,000.00**.

Figure 3: Email scam of World Cup-related lottery wins (Sourced from ESET "You have NOT won! A look at fake FIFA World Cup-themed lotteries and giveaways (*7-2)")

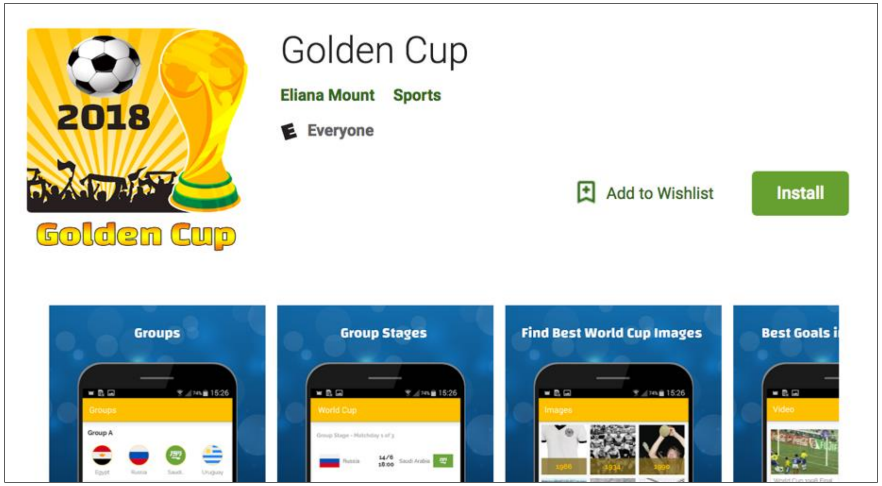
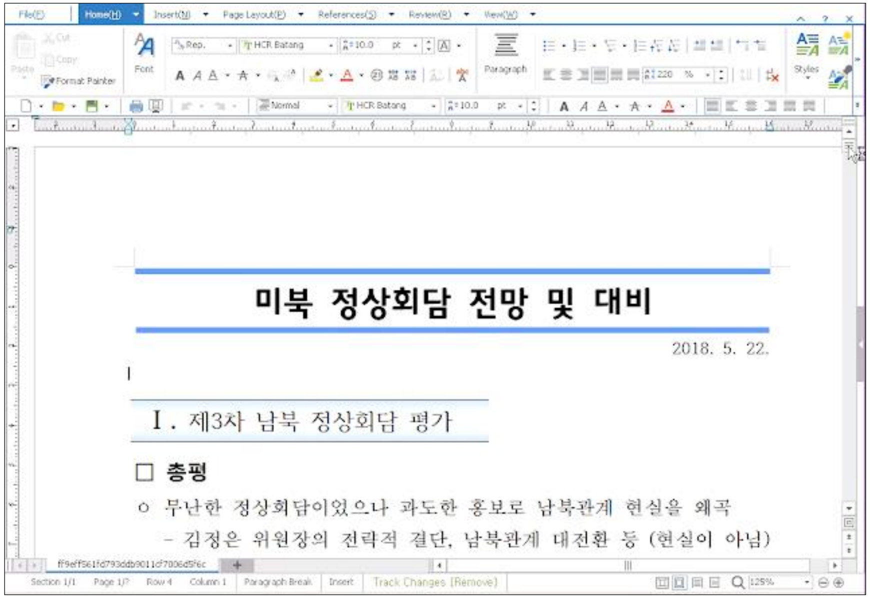


Figure 4: Malware disguised as a news flash app for the game results (Sourced from Symantec "GoldenCup: New Cyber Threat Targeting World Cup Fans (*7-4)")

# I. Hot Topic (11/11)
# (7) Cyber attacks related to international events

## (7-2) North Korea-United States Summit in Singapore

- On May 31, Cisco Talos found malware disguised as a document related to the North Korea-United States summit in Singapore which was to be held on June 12. This document was created in a form of "Araea Han-geul", word processor software holding the top share in South Korea, and intended to install a remote access tool NavRAT. The malware was communicating with the C&C server via NAVER email platform, the largest Korean Internet search portal website (*7-5).



미북 정상회담 전망 및 대비

2018. 5. 22.

Ⅰ. 제3차 남북 정상회담 평가

□ 총평

ㅇ 무난한 정상회담이었으나 과도한 홍보로 남북관계 현실을 왜곡

- 김정은 위원장의 전략적 결단, 남북관계 대전환 등 (현실이 아님)

Figure 5: Hangul document disguised as a summit-related document (Sourced from Cisco "NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea (*7-5)")

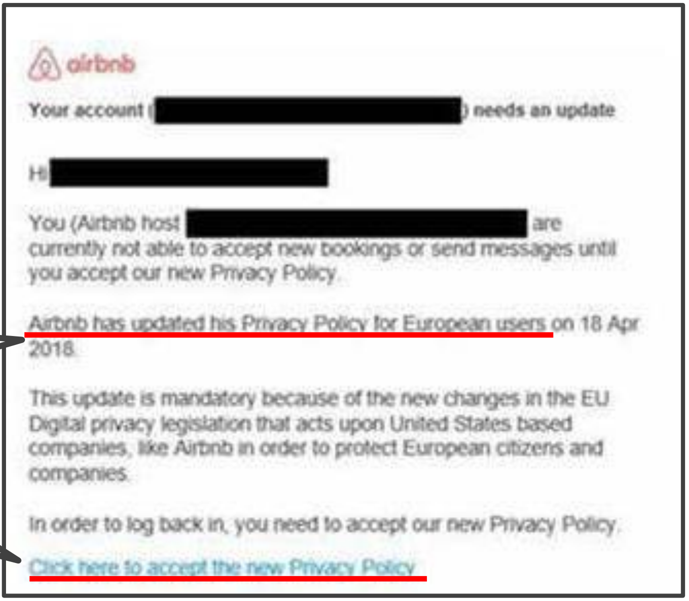
- On June 4, FireEye announced analytical results indicating that a North Korea hacking group APT37 and a Chinese group are exchanging information on cyber attacks. APT37 is continuously spying South Korea, aiming to steal foreign policy information of the South Korean government (*7-6).

# II. Forecast (1/2)

## (1) Spread of cyber attacks related to the GDPR

- Companies violating the GDPR are fined up to 4% of their annual sales or 20 million Euros as penalty. Cyber criminals may exploit this regulation to threaten companies. For example, the following scenarios are assumed.
  1. A cyber criminal steals personal information from a company handling EU residents' personal information.
  2. The criminal shows the company a part of information that he has stolen and threatens to leak the information unless the company pays money.
  3. If the company fails to notify the competent authority about it in time, the criminal requests a larger amount of money bringing up the penalty.

- Phishing scams requesting compliance with the GDPR to stir feelings of anxiety and GDPR-themed business email scams may spread widely. Using the regulation which obliges companies to notify the information leakage to the competent authority within 72 hours, the criminal may encourage companies to hasten the payment.



Your account ([redacted]) needs an update

Hi [redacted]

You (Airbnb host [redacted] are currently not able to accept new bookings or send messages until you accept our new Privacy Policy.

Airbnb has updated his Privacy Policy for European users on 18 Apr 2018.

This update is mandatory because of the new changes in the EU Digital privacy legislation that acts upon United States based companies, like Airbnb in order to protect European citizens and companies.

In order to log back in, you need to accept our new Privacy Policy.

Click here to accept the new Privacy Policy

It is described that the privacy policy for EU residents has been updated.

Clicking the link will lead to a malicious website.

Figure 6: Phishing email disguised as Airbnb to request agreement on the privacy policy
(Sourced from Redscan "REDSCAN IN THE NEWS: RAISING AWARENESS OF GDPR PHISHING SCAMS (*8-1)")

# II. Forecast (2/2)

### (2) New targets for cryptocurrency mining software

Cyber attackers are more likely to aim for acquiring cryptocurrencies fraudulently as a means to make profits more reliably than ransomware. Meanwhile, however, software for mining cryptocurrencies fraudulently, “miner”, is now being increasingly detected by anti-virus software and excluded from official application stores. It is now getting difficult to mine cryptocurrencies using private personal computers and smart phones.

On the other hand, while companies are accelerating the use of cloud services, security measures for them tend to be reactive. It is expected that attacks will increase where attackers fraudulently login to an account using vulnerabilities and faulty settings of the cloud environment such as Kubernetes where the construction and operation have been automated, and install software for mining cryptocurrencies to carry out a large-scale fraudulent mining.

### (3) Cyber attacks related to political events during Q2 to Q3 in FY2018

- In relation to the trade friction between the US and China, cyber attacks may get overheated between the two countries.
- In relation to the midterm election in the US on November 6, risk of cyber attacks on election systems will increase. Also, fake news targeting manipulation of the election may circulate as in the 2016 presidential election.

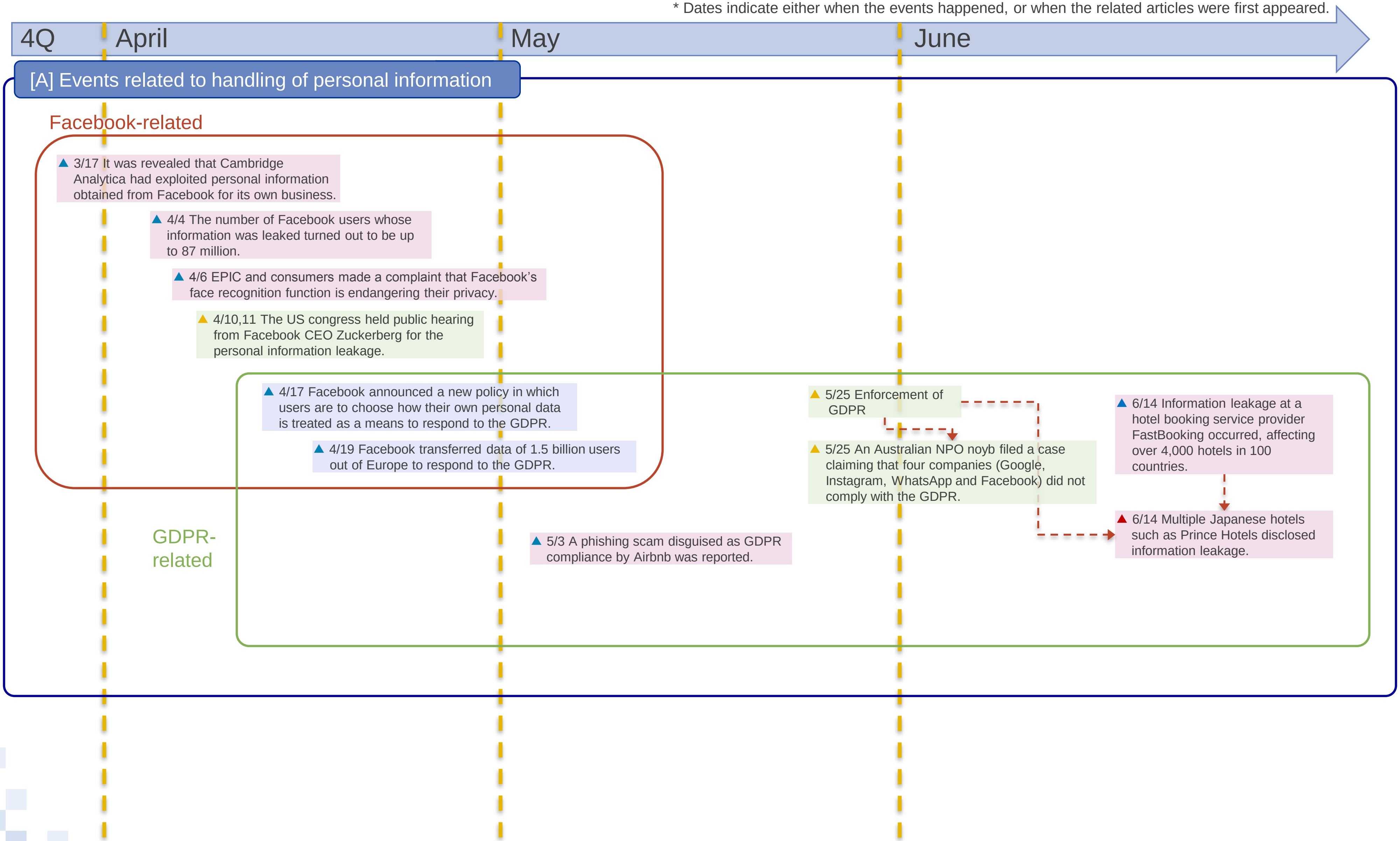
# III. Timeline (1/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan

🟨: Vulnerabilities
🟧: Threats
🟪: Cyber attacks/incidents

🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



[A] Events related to handling of personal information

Facebook-related

▲ 3/17 It was revealed that Cambridge Analytica had exploited personal information obtained from Facebook for its own business.

▲ 4/4 The number of Facebook users whose information was leaked turned out to be up to 87 million.

▲ 4/6 EPIC and consumers made a complaint that Facebook’s face recognition function is endangering their privacy.

▲ 4/10,11 The US congress held public hearing from Facebook CEO Zuckerberg for the personal information leakage.

▲ 4/17 Facebook announced a new policy in which users are to choose how their own personal data is treated as a means to respond to the GDPR.

▲ 4/19 Facebook transferred data of 1.5 billion users out of Europe to respond to the GDPR.

GDPR-related

▲ 5/3 A phishing scam disguised as GDPR compliance by Airbnb was reported.

▲ 5/25 Enforcement of GDPR

▲ 5/25 An Australian NPO noyb filed a case claiming that four companies (Google, Instagram, WhatsApp and Facebook) did not comply with the GDPR.

▲ 6/14 Information leakage at a hotel booking service provider FastBooking occurred, affecting over 4,000 hotels in 100 countries.

▲ 6/14 Multiple Japanese hotels such as Prince Hotels disclosed information leakage.

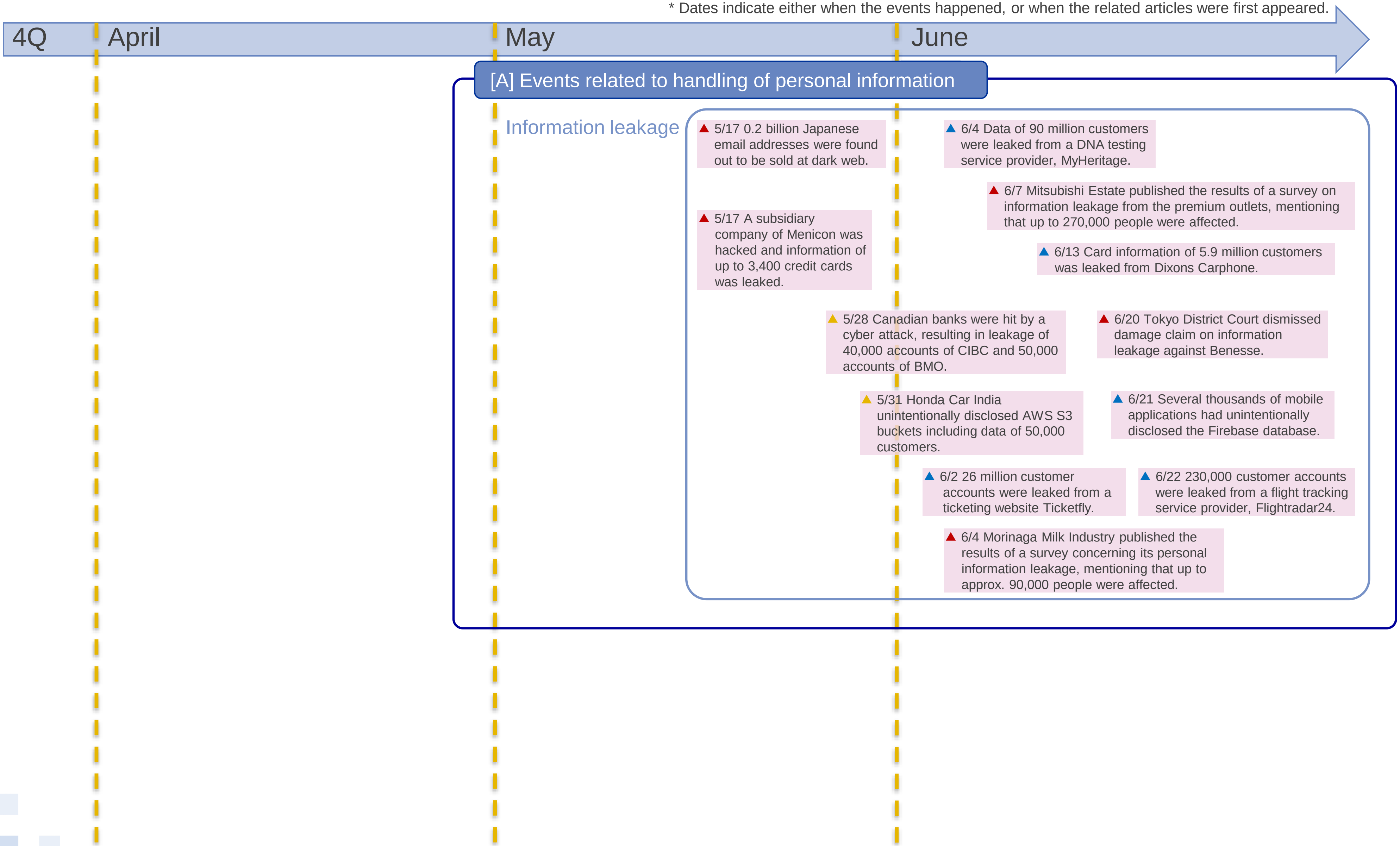
# III. Timeline (2/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan

🟨: Vulnerabilities
🟧: Threats
🟪: Cyber attacks/incidents

🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



[A] Events related to handling of personal information

Information leakage

▲ 5/17 0.2 billion Japanese email addresses were found out to be sold at dark web.

▲ 5/17 A subsidiary company of Menicon was hacked and information of up to 3,400 credit cards was leaked.

▲ 5/28 Canadian banks were hit by a cyber attack, resulting in leakage of 40,000 accounts of CIBC and 50,000 accounts of BMO.

▲ 5/31 Honda Car India unintentionally disclosed AWS S3 buckets including data of 50,000 customers.

▲ 6/2 26 million customer accounts were leaked from a ticketing website Ticketfly.

▲ 6/4 Data of 90 million customers were leaked from a DNA testing service provider, MyHeritage.

▲ 6/4 Morinaga Milk Industry published the results of a survey concerning its personal information leakage, mentioning that up to approx. 90,000 people were affected.

▲ 6/7 Mitsubishi Estate published the results of a survey on information leakage from the premium outlets, mentioning that up to 270,000 people were affected.

▲ 6/13 Card information of 5.9 million customers was leaked from Dixons Carphone.

▲ 6/20 Tokyo District Court dismissed damage claim on information leakage against Benesse.

▲ 6/21 Several thousands of mobile applications had unintentionally disclosed the Firebase database.

▲ 6/22 230,000 customer accounts were leaked from a flight tracking service provider, Flightradar24.

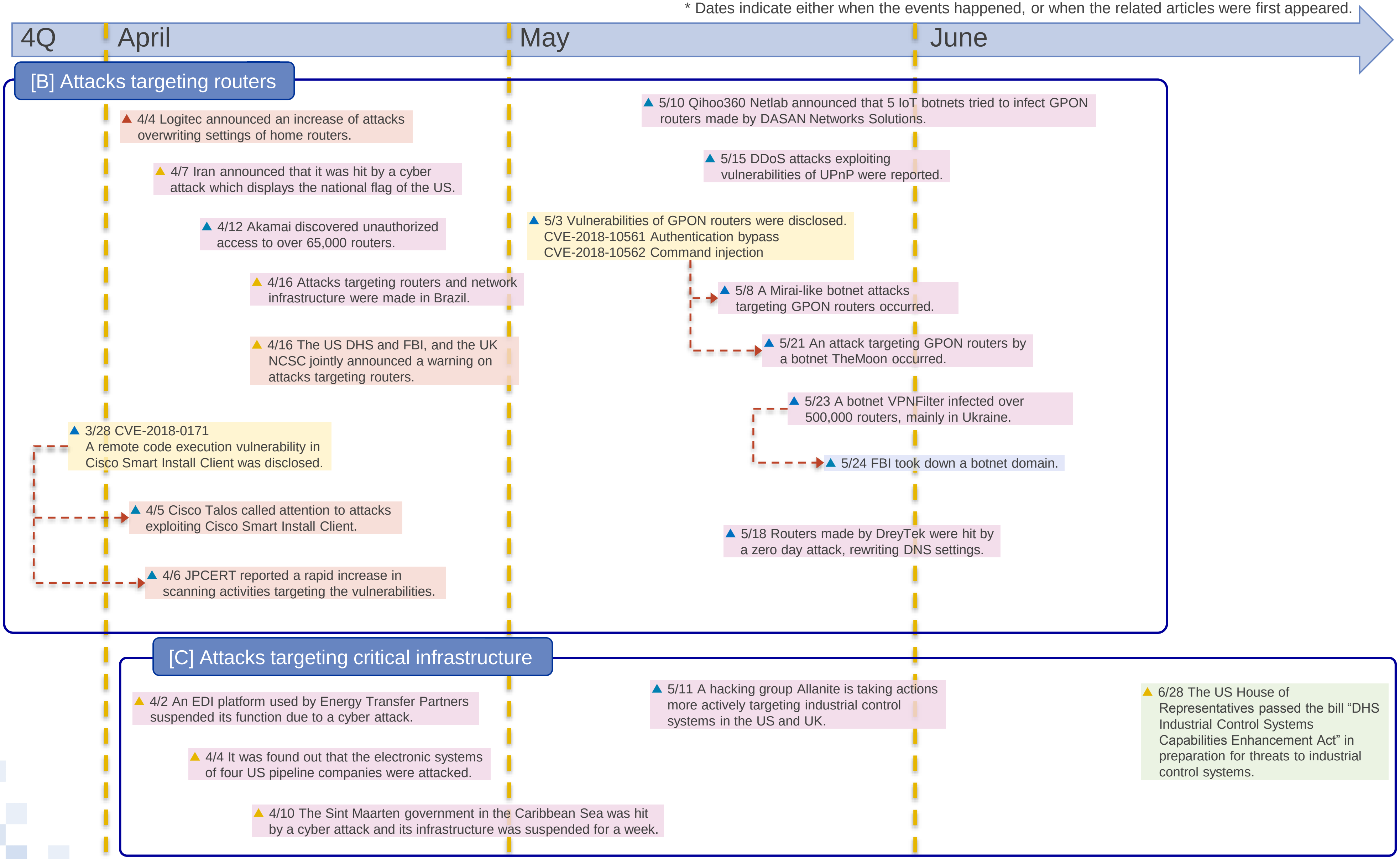
# III. Timeline (3/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan

🟨: Vulnerabilities
🟧: Threats
🟪: Cyber attacks/incidents

🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



## [B] Attacks targeting routers

▲ 4/4 Logitec announced an increase of attacks overwriting settings of home routers.

▲ 4/7 Iran announced that it was hit by a cyber attack which displays the national flag of the US.

▲ 4/12 Akamai discovered unauthorized access to over 65,000 routers.

▲ 4/16 Attacks targeting routers and network infrastructure were made in Brazil.

▲ 4/16 The US DHS and FBI, and the UK NCSC jointly announced a warning on attacks targeting routers.

▲ 3/28 CVE-2018-0171
A remote code execution vulnerability in Cisco Smart Install Client was disclosed.

▲ 4/5 Cisco Talos called attention to attacks exploiting Cisco Smart Install Client.

▲ 4/6 JPCERT reported a rapid increase in scanning activities targeting the vulnerabilities.

▲ 5/10 Qihoo360 Netlab announced that 5 IoT botnets tried to infect GPON routers made by DASAN Networks Solutions.

▲ 5/15 DDoS attacks exploiting vulnerabilities of UPnP were reported.

▲ 5/3 Vulnerabilities of GPON routers were disclosed.
CVE-2018-10561 Authentication bypass
CVE-2018-10562 Command injection

▲ 5/8 A Mirai-like botnet attacks targeting GPON routers occurred.

▲ 5/21 An attack targeting GPON routers by a botnet TheMoon occurred.

▲ 5/23 A botnet VPNFilter infected over 500,000 routers, mainly in Ukraine.

▲ 5/24 FBI took down a botnet domain.

▲ 5/18 Routers made by DreyTek were hit by a zero day attack, rewriting DNS settings.

## [C] Attacks targeting critical infrastructure

▲ 4/2 An EDI platform used by Energy Transfer Partners suspended its function due to a cyber attack.

▲ 4/4 It was found out that the electronic systems of four US pipeline companies were attacked.

▲ 4/10 The Sint Maarten government in the Caribbean Sea was hit by a cyber attack and its infrastructure was suspended for a week.

▲ 5/11 A hacking group Allanite is taking actions more actively targeting industrial control systems in the US and UK.

▲ 6/28 The US House of Representatives passed the bill "DHS Industrial Control Systems Capabilities Enhancement Act" in preparation for threats to industrial control systems.

# III. Timeline (4/10)

▲: Globally common ■: Vulnerabilities ■: Countermeasures
▲: Specific regional ■: Threats ■: Governments
▲: Domestic in Japan ■: Cyber attacks/incidents

* Dates indicate either when the events happened, or when the related articles were first appeared.

4Q | April | May | June

## [D] Cryptocurrencies

▲ 2017/3/26 CVE-2017-7269
A remote code execution vulnerability in IIS 6.0 due to buffer overflows was disclosed.

▲ 4/12 An attack for mining cryptocurrency Electroneum occurred.

▲ 4/2 Malware njRAT was additionally equipped with ransomware and a function to steal cryptocurrencies.

▲ 4/9 Fraudulent mining was carried out for cryptocurrency Verge exploiting defects of software.

▲ 4/13 Cryptocurrency equivalent to 3 million dollars was stolen from a major Indian cryptocurrency exchange Coinsecure.

▲ 4/17 Ransomware XIAOBA was equipped with a function to mine cryptocurrencies.

▲ 4/23 TrendMicro discovered a new variant of worm RETADUP that mines cryptocurrency Monero.

▲ 5/11 A botnet Satori mass-scanned the Ethereum mining software.

▲ 5/17 Malware WinstarNssmMine infected over 500,000 PCs within 3 days to mine cryptocurrencies.

▲ 5/17 Cryptocurrency Monacoin was hit by a 51% attack.

▲ 5/18 Bitcoin Gold was hit by a 51% attack, allowing the attacker to fraudulently get 18 million dollars through double-spending transactions.

▲ 5/23 Cryptocurrency Verge was hit by a 51% attack again.

▲ 5/28 A remote code execution vulnerability was discovered in the EOS blockchain.

▲ 5/28 Cryptocurrency transaction application Taylor suffered a theft of 1.5 million dollars of cryptocurrency.

▲ 6/10 A Korean exchange Coinrail was hacked, with ICO token equivalent to 40 million dollars stolen.

▲ 6/11 Cyber attackers made profit of over 20 million dollars from an attack targeting an Ethereum mining node.

▲ 6/12 5% of cryptocurrency Monero flows was found to be mined by malware.

▲ 6/15 Malware fraudulently operating a clipboard to steal cryptocurrencies infected over 3 million machines.

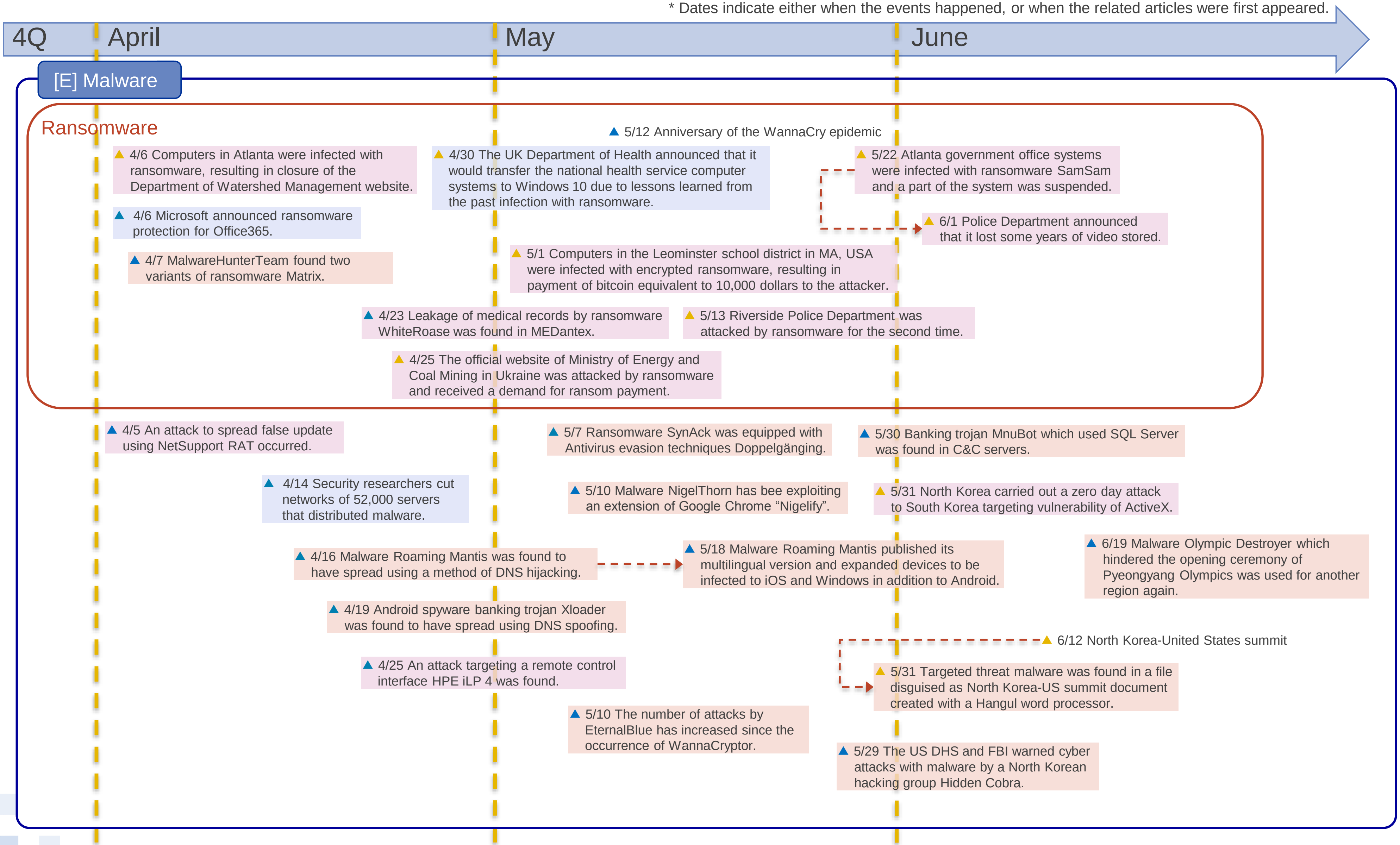
▲ 6/18 Malware to mine cryptocurrencies targeting Amazon Fire TV and Fire TV Stick was found.

▲ 6/24 A Korean exchange Bithumb was hacked, with cryptocurrency equivalent to 31 million dollars stolen.

# III. Timeline (5/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan
🟨: Vulnerabilities
🟧: Threats
🟪: Cyber attacks/incidents
🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



## [E] Malware

### Ransomware

▲ 5/12 Anniversary of the WannaCry epidemic

▲ 4/6 Computers in Atlanta were infected with ransomware, resulting in closure of the Department of Watershed Management website.

▲ 4/6 Microsoft announced ransomware protection for Office365.

▲ 4/7 MalwareHunterTeam found two variants of ransomware Matrix.

▲ 4/23 Leakage of medical records by ransomware WhiteRoase was found in MEDantex.

▲ 4/25 The official website of Ministry of Energy and Coal Mining in Ukraine was attacked by ransomware and received a demand for ransom payment.

▲ 4/30 The UK Department of Health announced that it would transfer the national health service computer systems to Windows 10 due to lessons learned from the past infection with ransomware.

▲ 5/1 Computers in the Leominster school district in MA, USA were infected with encrypted ransomware, resulting in payment of bitcoin equivalent to 10,000 dollars to the attacker.

▲ 5/13 Riverside Police Department was attacked by ransomware for the second time.

▲ 5/22 Atlanta government office systems were infected with ransomware SamSam and a part of the system was suspended.

▲ 6/1 Police Department announced that it lost some years of video stored.

▲ 4/5 An attack to spread false update using NetSupport RAT occurred.

▲ 4/14 Security researchers cut networks of 52,000 servers that distributed malware.

▲ 4/16 Malware Roaming Mantis was found to have spread using a method of DNS hijacking.

▲ 4/19 Android spyware banking trojan Xloader was found to have spread using DNS spoofing.

▲ 4/25 An attack targeting a remote control interface HPE iLP 4 was found.

▲ 5/7 Ransomware SynAck was equipped with Antivirus evasion techniques Doppelgänging.

▲ 5/10 Malware NigelThorn has bee exploiting an extension of Google Chrome “Nigelify”.

▲ 5/18 Malware Roaming Mantis published its multilingual version and expanded devices to be infected to iOS and Windows in addition to Android.

▲ 5/10 The number of attacks by EternalBlue has increased since the occurrence of WannaCryptor.

▲ 5/30 Banking trojan MnuBot which used SQL Server was found in C&C servers.

▲ 5/31 North Korea carried out a zero day attack to South Korea targeting vulnerability of ActiveX.

▲ 6/19 Malware Olympic Destroyer which hindered the opening ceremony of Pyeongyang Olympics was used for another region again.

▲ 6/12 North Korea-United States summit

▲ 5/31 Targeted threat malware was found in a file disguised as North Korea-US summit document created with a Hangul word processor.

▲ 5/29 The US DHS and FBI warned cyber attacks with malware by a North Korean hacking group Hidden Cobra.

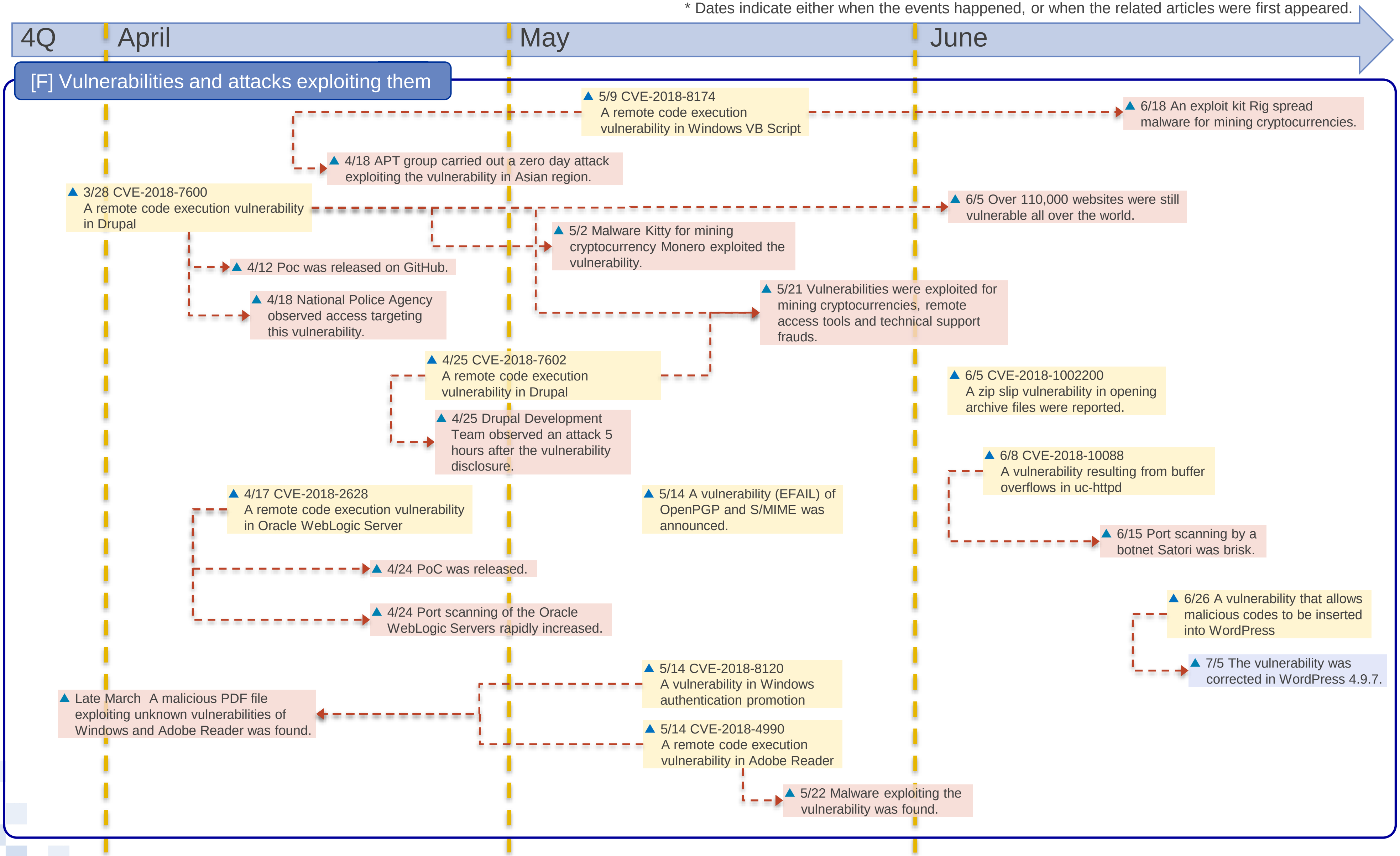
# III. Timeline (6/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan

🟨: Vulnerabilities
🟥: Threats
🟪: Cyber attacks/incidents

🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



## [F] Vulnerabilities and attacks exploiting them

▲ 3/28 CVE-2018-7600
A remote code execution vulnerability in Drupal

▲ 4/12 Poc was released on GitHub.

▲ 4/18 National Police Agency observed access targeting this vulnerability.

▲ 5/2 Malware Kitty for mining cryptocurrency Monero exploited the vulnerability.

▲ 6/5 Over 110,000 websites were still vulnerable all over the world.

▲ 5/9 CVE-2018-8174
A remote code execution vulnerability in Windows VB Script

▲ 4/18 APT group carried out a zero day attack exploiting the vulnerability in Asian region.

▲ 6/18 An exploit kit Rig spread malware for mining cryptocurrencies.

▲ 4/25 CVE-2018-7602
A remote code execution vulnerability in Drupal

▲ 4/25 Drupal Development Team observed an attack 5 hours after the vulnerability disclosure.

▲ 5/21 Vulnerabilities were exploited for mining cryptocurrencies, remote access tools and technical support frauds.

▲ 4/17 CVE-2018-2628
A remote code execution vulnerability in Oracle WebLogic Server

▲ 4/24 PoC was released.

▲ 4/24 Port scanning of the Oracle WebLogic Servers rapidly increased.

▲ 5/14 A vulnerability (EFAIL) of OpenPGP and S/MIME was announced.

▲ 5/14 CVE-2018-8120
A vulnerability in Windows authentication promotion

▲ 5/14 CVE-2018-4990
A remote code execution vulnerability in Adobe Reader

▲ Late March A malicious PDF file exploiting unknown vulnerabilities of Windows and Adobe Reader was found.

▲ 5/22 Malware exploiting the vulnerability was found.

▲ 6/5 CVE-2018-1002200
A zip slip vulnerability in opening archive files were reported.

▲ 6/8 CVE-2018-10088
A vulnerability resulting from buffer overflows in uc-httpd

▲ 6/15 Port scanning by a botnet Satori was brisk.

▲ 6/26 A vulnerability that allows malicious codes to be inserted into WordPress

▲ 7/5 The vulnerability was corrected in WordPress 4.9.7.

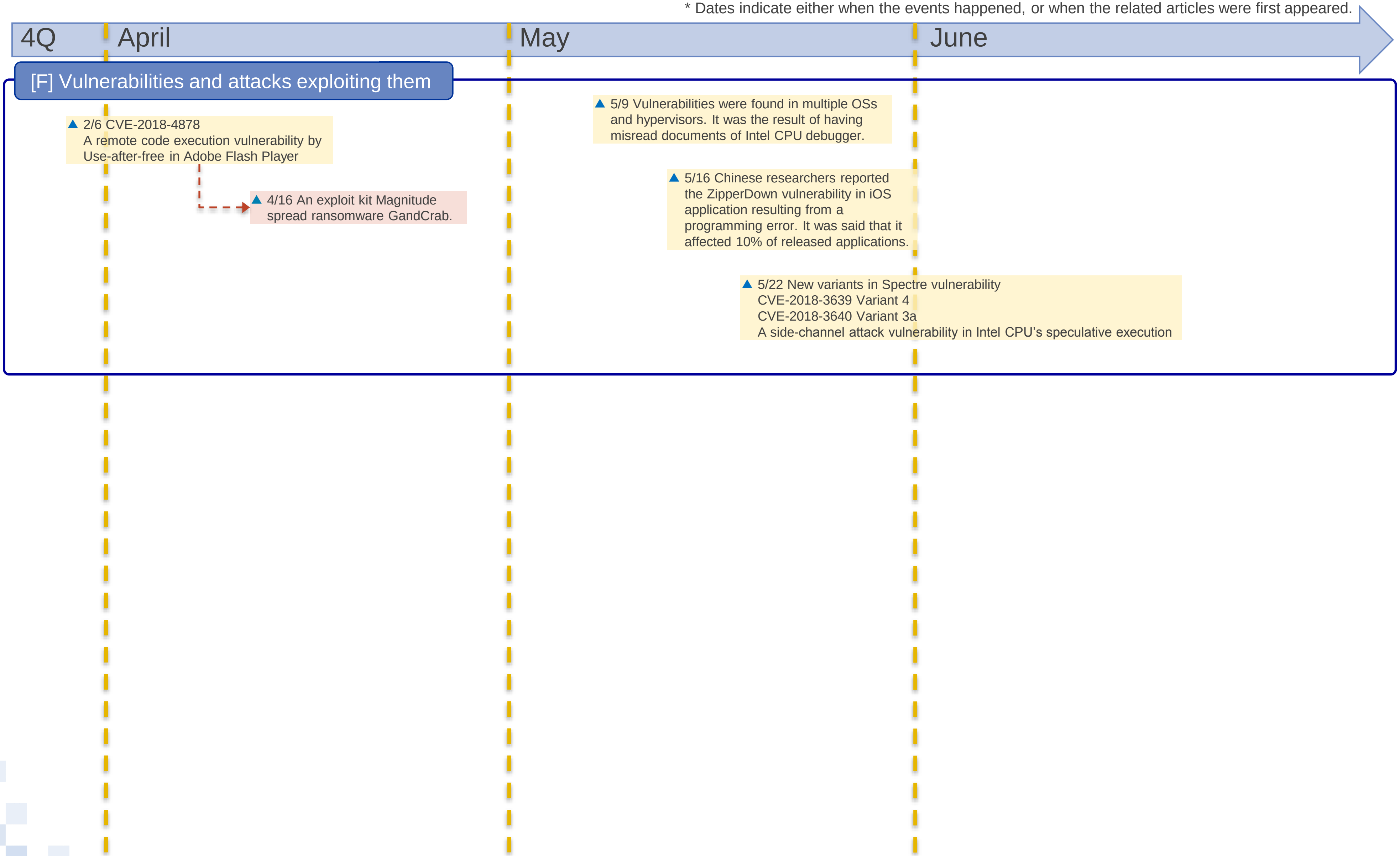
# III. Timeline (7/10)

▲: Globally common ▲: Specific regional ▲: Domestic in Japan

🟨: Vulnerabilities 🟥: Threats 🟪: Cyber attacks/incidents

🟦: Countermeasures 🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



4Q April May June

[F] Vulnerabilities and attacks exploiting them

▲ 2/6 CVE-2018-4878
A remote code execution vulnerability by Use-after-free in Adobe Flash Player

▲ 4/16 An exploit kit Magnitude spread ransomware GandCrab.

▲ 5/9 Vulnerabilities were found in multiple OSs and hypervisors. It was the result of having misread documents of Intel CPU debugger.

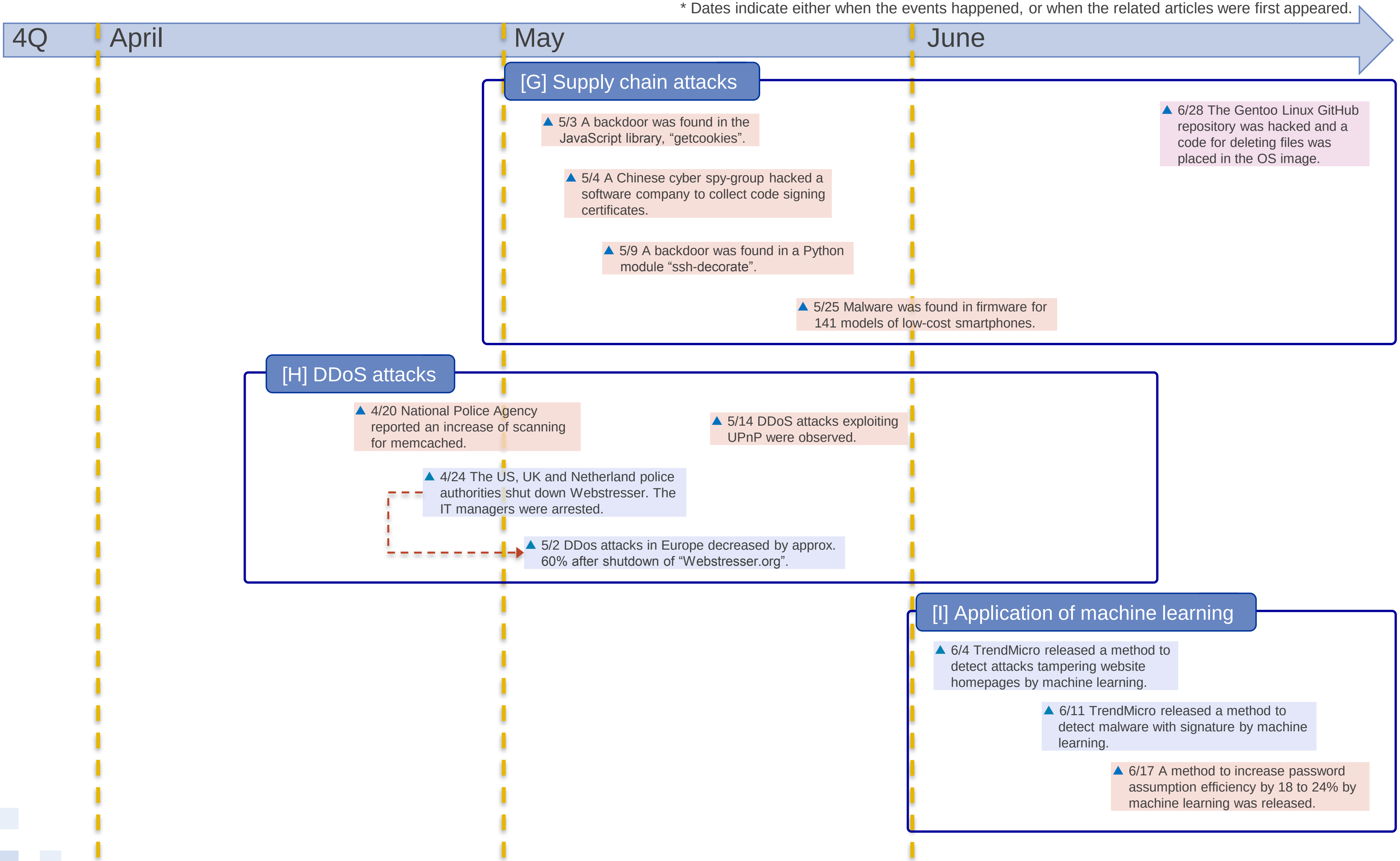
▲ 5/16 Chinese researchers reported the ZipperDown vulnerability in iOS application resulting from a programming error. It was said that it affected 10% of released applications.

▲ 5/22 New variants in Spectre vulnerability
CVE-2018-3639 Variant 4
CVE-2018-3640 Variant 3a
A side-channel attack vulnerability in Intel CPU's speculative execution

# III. Timeline (8/10)

▲: Globally common ■: Vulnerabilities ■: Countermeasures
▲: Specific regional ■: Threats ■: Governments
▲: Domestic in Japan ■: Cyber attacks/incidents

* Dates indicate either when the events happened, or when the related articles were first appeared.



4Q

April

May

June

## [G] Supply chain attacks

▲ 5/3 A backdoor was found in the JavaScript library, “getcookies”.

▲ 5/4 A Chinese cyber spy-group hacked a software company to collect code signing certificates.

▲ 5/9 A backdoor was found in a Python module “ssh-decorate”.

▲ 5/25 Malware was found in firmware for 141 models of low-cost smartphones.

▲ 6/28 The Gentoo Linux GitHub repository was hacked and a code for deleting files was placed in the OS image.

## [H] DDoS attacks

▲ 4/20 National Police Agency reported an increase of scanning for memcached.

▲ 4/24 The US, UK and Netherland police authorities shut down Webstresser. The IT managers were arrested.

▲ 5/2 DDos attacks in Europe decreased by approx. 60% after shutdown of “Webstresser.org”.

▲ 5/14 DDoS attacks exploiting UPnP were observed.

## [I] Application of machine learning

▲ 6/4 TrendMicro released a method to detect attacks tampering website homepages by machine learning.

▲ 6/11 TrendMicro released a method to detect malware with signature by machine learning.

▲ 6/17 A method to increase password assumption efficiency by 18 to 24% by machine learning was released.

# III. Timeline (9/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan
🟨: Vulnerabilities
🟥: Threats
🟪: Cyber attacks/incidents
🟦: Countermeasures
🟩: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.

4Q | April | May | June

## [J] Efforts made by the government and public agencies

▲ 4/2 NIST published a draft of “Precautions for managing IoT security and privacy risks for federal information systems”.

▲ 4/2 Japan Business Federation announced consolidation of measures against cyber attacks in Tokyo Olympic Games.

▲ 4/2 Metropolitan Police Department integrated departments responding to cyber attacks and cyber crimes into one.

▲ 4/4 The government summarized the outline of “Cybersecurity Strategy”.

▲ 4/19 Ministry of Land, Infrastructure, Transport and Tourism decided to support establishment of “Auto-ISAC (tentative)” consisting of approx. 60 related companies and organizations in Japan.

▲ 4/25 IPA summarized outcomes in “Non-Functional Requirements Grade Revision Working Group” and released “Non-Functional Requirements Grades 2018”.

▲ 4/27 ASEAN agreed to consolidate in the filed of cyber protection.

▲ 5/4 NIST published the “Platform Firmware Resiliency Guidelines”.

▲ 5/6 The government decided to dispatch officers from the Ministry of Defense to Estonia to consolidate cooperation relation in the cyber field.

▲ 5/29 Europol gathered members from the law enforcement agency to establish a dark web investigation team.

▲ 5/30 IPA published a “Guideline for methods of selecting forms of management when opening websites, etc.”

▲ 6/7 The government summarized cybersecurity strategy plans up to 2021 and decided to support development of a quantum computer, AI and cryptographic technology resistant to cyber attacks.

▲ 6/15 Ministry of Economy, Trade and Industry and IPA established a “collaboration platform” to exchange information on cybersecurity measures.

▲ 6/15 IPA published a “Guideline for methods of selecting forms of management when opening websites, etc.”

## [K] Attacks on financial institutions

▲ 4/30 A Mexican bank was hit by a cyber attack and over 0.3 billion pesos were stolen.

▲ 5/24 A Chilean bank was attacked by a wiper KillDisk, resulting in suspension of its system.

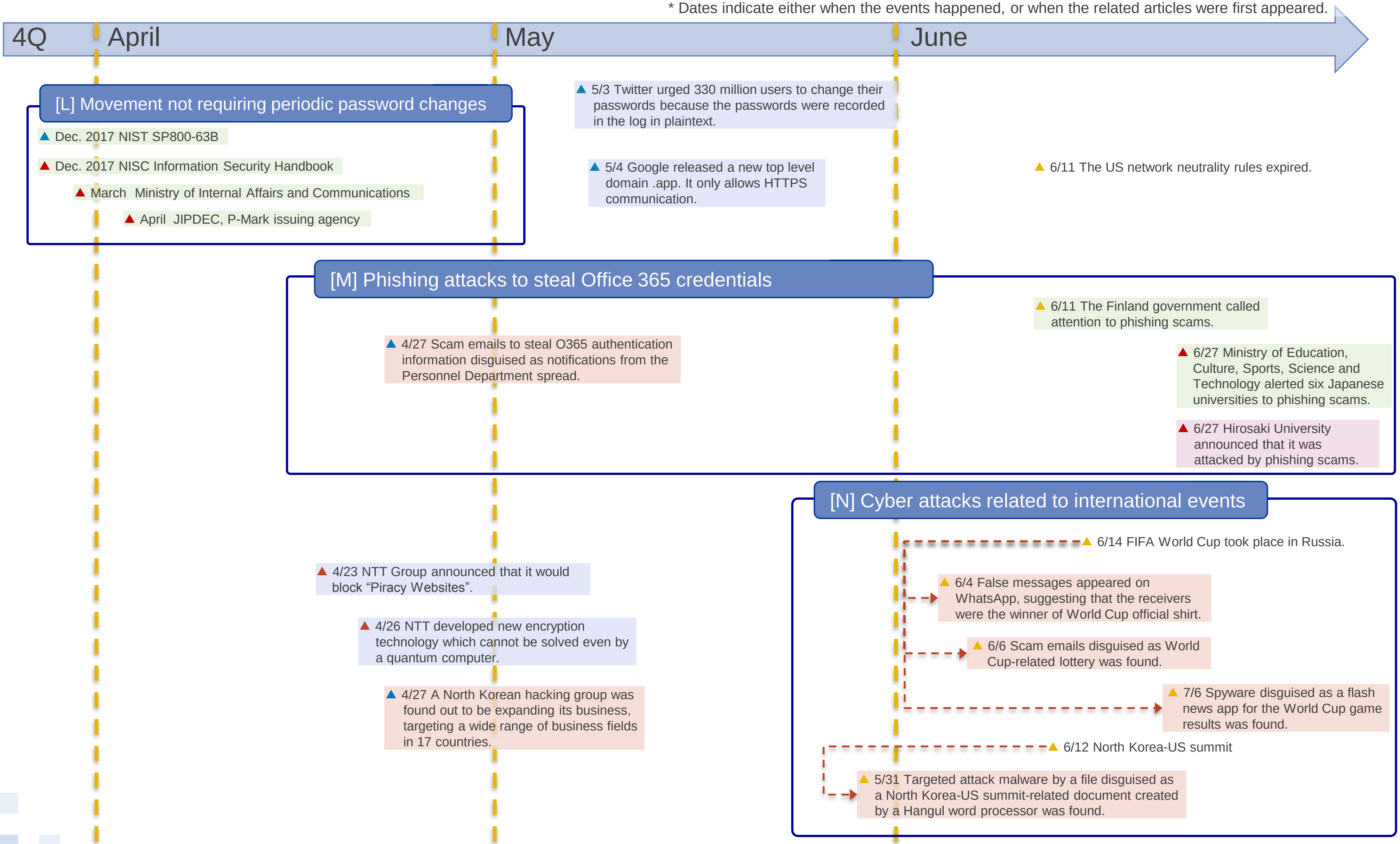
# III. Timeline (10/10)

▲: Globally common
▲: Specific regional
▲: Domestic in Japan

■: Vulnerabilities
■: Threats
■: Cyber attacks/incidents

■: Countermeasures
■: Governments

* Dates indicate either when the events happened, or when the related articles were first appeared.



## [L] Movement not requiring periodic password changes

▲ Dec. 2017 NIST SP800-63B

▲ Dec. 2017 NISC Information Security Handbook

▲ March Ministry of Internal Affairs and Communications

▲ April JIPDEC, P-Mark issuing agency

▲ 5/3 Twitter urged 330 million users to change their passwords because the passwords were recorded in the log in plaintext.

▲ 5/4 Google released a new top level domain .app. It only allows HTTPS communication.

▲ 6/11 The US network neutrality rules expired.

## [M] Phishing attacks to steal Office 365 credentials

▲ 4/27 Scam emails to steal O365 authentication information disguised as notifications from the Personnel Department spread.

▲ 6/11 The Finland government called attention to phishing scams.

▲ 6/27 Ministry of Education, Culture, Sports, Science and Technology alerted six Japanese universities to phishing scams.

▲ 6/27 Hirosaki University announced that it was attacked by phishing scams.

▲ 4/23 NTT Group announced that it would block “Piracy Websites”.

▲ 4/26 NTT developed new encryption technology which cannot be solved even by a quantum computer.

▲ 4/27 A North Korean hacking group was found out to be expanding its business, targeting a wide range of business fields in 17 countries.

## [N] Cyber attacks related to international events

▲ 6/14 FIFA World Cup took place in Russia.

▲ 6/4 False messages appeared on WhatsApp, suggesting that the receivers were the winner of World Cup official shirt.

▲ 6/6 Scam emails disguised as World Cup-related lottery was found.

▲ 7/6 Spyware disguised as a flash news app for the World Cup game results was found.

▲ 6/12 North Korea-US summit

▲ 5/31 Targeted attack malware by a file disguised as a North Korea-US summit-related document created by a Hangul word processor was found.

# Revised history

| Revised date | Pag e | Revised part | Revised contents |
|---|---|---|---|
| November 20th, 2018 | 8 | (2-2) Attacks targeting routers for consumers | We found the following error and fixed it.<br>(Error)Malware VPNFilter infected routers made by Logitec and Buffalo.<br>(Correct)Malware Roaming Mantis infected routers made by Logitec and Buffalo. |

# References(1/3)

(*1-1) Help! GDPR or Phishing Mail? | Avira https://blog.avira.com/help-gdpr-or-phishing-mail/

(*1-2) GoogleとFacebook、GDPR施行初日にさっそく提訴される | ITmedia http://www.itmedia.co.jp/news/articles/1805/27/news011.html

(*1-3) プリンスホテルの委託先サイトに不正アクセス、12.5万件の情報漏えい | ZDNet https://japan.zdnet.com/article/35121487/

(*1-4) Trump campaign-linked data firm Cambridge Analytica reportedly collected info on 50M Facebook profiles | TechCrunch https://techcrunch.com/2018/03/17/trump-campaign-linked-data-firm-cambridge-analytica-reportedly-collected-info-on-50m-facebook-profiles/

(*1-5) An Update on Our Plans to Restrict Data Access on Facebook | Facebook https://newsroom.fb.com/news/2018/04/restricting-data-access/

(*1-6) フェイスブックＣＥＯ「私の過ち」 米議会で謝罪 | 日経 https://www.nikkei.com/article/DGXMZO29242870R10C18A4000000/

(*2-1) Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client | Cisco https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html

(*2-2) Cisco Smart Install プロトコルを狙った攻撃の急増 | NICTER http://blog.nicter.jp/reports/2018-03/cisco-switch-hack/

(*2-3) Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices | NCSC https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

(*2-4) ネットワーク機器を狙う IoT ボット「VPNFilter」、世界で 50 万台以上に感染 | TrendMicro https://blog.trendmicro.co.jp/archives/17484

(*2-5) DNS設定を乗っ取りAndroidデバイスに感染するRoaming Mantis | Kaspersky https://blog.kaspersky.co.jp/roaming-mantis/20105/

(*2-6) ルーターへのサイバー攻撃相次ぐ 個人情報盗む目的か | 日経 https://www.nikkei.com/article/DGXMZO29079420W8A400C1CR0000/

(*2-7) IoTサイバー攻撃情報を事業者間で共有、総務省が国会に改正法案を提出 | TrendMicro https://www.trendmicro.com/jp/iot-security/news/20157

# References(2/3)

(*3-1) Cryptocurrency trading app Taylor says all funds have been stolen in cyberattack | ZDNet https://www.zdnet.com/article/all-of-cryptocurrency-trading-app-taylors-funds-have-been-stolen/

(*3-2) Hacker mines up to $1 million in Verge after exploiting major bug | Sophos https://nakedsecurity.sophos.com/2018/04/09/hacker-mines-up-to-1-million-in-verge-after-exploiting-major-bug/

(*3-3) South Korean Cryptocurrency Exchange Coinrail hacked, hackers stole over $40M worth of ICO tokens | Security Affairs https://securityaffairs.co/wordpress/73426/cyber-crime/cryptocurrency-exchange-coinrail-hacked.html

(*3-4) Bithumb $31 Million Crypto Exchange Hack: What We Know (And Don't) | CoinDesk https://www.coindesk.com/bithumb-exchanges-31-million-hack-know-dont-know/

(*3-5) WinstarNssmMiner Coinminer Campaign Makes 500,000 Victims in Three Days | Bleeping Computer https://www.bleepingcomputer.com/news/security/winstarnssmminer-coinminer-campaign-makes-500-000-victims-in-three-days/

(*3-6) Amazon Fire TV and the ADB.Miner malware ? what you need to know | CordCutters https://www.cordcutters.com/amazon-fire-tv-and-adbminer-malware-what-you-need-know

(*4-1) One year later: EternalBlue exploit more popular now than during WannaCryptor outbreak | ESET https://www.welivesecurity.com/2018/05/10/one-year-later-eternalblue-exploit-wannacryptor/

(*4-2) New Satan Ransomware available through a Ransomware as a Service. | Bleeping Computer https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/

(*4-3) Satan ransomware adds EternalBlue exploit |Blaze's Security Blog https://bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html

(*4-4) Satan Ransomware Spawns New Methods to Spread | AlienVault https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread

(*4-5) DBGer Ransomware Uses EternalBlue and Mimikatz to Spread Across Networks | Bleeping Computer https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/

(*4-6) 「CERBER」バージョン6：ランサムウェアの変遷と今後の展開 | TrendMicro https://blog.trendmicro.co.jp/archives/15054

(*4-7) ランサムウェア「CERBER」に新たな機能追加。ビットコインを窃取 | TrendMicro https://blog.trendmicro.co.jp/archives/15664

# References(3/3)

(*5-1) Reported malicious module: getcookies | The npm Blog https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

(*5-2) Backdoored Python Library Caught Stealing SSH Credentials | Bleeping Computer https://www.bleepingcomputer.com/news/security/backdoored-python-library-caught-stealing-ssh-credentials/

(*5-3) File-Wiping Malware Placed Inside Gentoo Linux Code After GitHub Account Hack | Bleeping Computer https://www.bleepingcomputer.com/news/linux/file-wiping-malware-placed-inside-gentoo-linux-code-after-github-account-hack/

(*5-4) Minecraft players exposed to malicious code in modified “skins” | Avast https://blog.avast.com/minecraft-players-exposed-to-malicious-code-in-modified-skins

(*5-5) MINECRAFT: JAVA EDITION SKINS ISSUE UPDATE | Minecraft https://minecraft.net/en-us/article/minecraft-java-edition-skins-issue-update

(*6-1) SP800-63B | NIST https://openid-foundation-japan.github.io/800-63-3/sp800-63b.ja.html

(*6-2) 情報セキュリティハンドブック | NISC https://www.nisc.go.jp/security-site/handbook/index.html

(*6-3) 「JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン-第2版-」の一部改訂について | JIPDECプライバシーマーク推進センター https://privacymark.jp/news/system/2018/0410.html

(*6-4) ヤフーがパスワードの定期変更求める記載削除へ　総務省も「安全なもの」前提呼びかけ | ITmedia http://www.itmedia.co.jp/news/articles/1804/24/news058.html

(*7-1) False contest to win jersey of the Brazilian team found on WhatsApp | ESET https://www.welivesecurity.com/2018/06/04/false-contest-win-brazilian-jersey-whatsapp/

(*7-2) You have NOT won! A look at fake FIFA World Cup-themed lotteries and giveaways | ESET https://www.welivesecurity.com/2018/06/06/fake-fifa-world-cup-themed-lotteries-giveaways/

(*7-3) 2018 Russia World Cup : Russian cyber spy may hack travelers’ mobile devices | Security Affairs https://securityaffairs.co/wordpress/73527/security/world-cup-survaillance.html

(*7-4) GoldenCup: New Cyber Threat Targeting World Cup Fans | Symantec https://www.symantec.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans

(*7-5) NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea | Cisco https://blog.talosintelligence.com/2018/05/navrat.html

(*7-6) 北朝鮮ハッカー集団「ＡＰＴ３７」、中国と連携　攻撃技術の情報交換　米朝会談見据えスパイ継続 | 産経ニュース https://www.sankei.com/world/news/180604/wor1806040019-n1.html

(*8-1) REDSCAN IN THE NEWS: RAISING AWARENESS OF GDPR PHISHING SCAMS | Redscan https://www.redscan.com/news/redscan-news-raising-awareness-gdpr-phishing-scams/

NTT DATA

Trusted Global Innovator