NTT DATA
Trusted Global Innovator

NTTDATA-CERT Global Security Quarterly Report: January - March 2018

May 23rd, 2018
NTT DATA Corporation

Table of Contents

Executive Summary

I. Hot Topic

II. Forecast

III. Timeline

References

Executive Summary

In FY2017Q4 (January - March 2018), the attacks targeting cryptocurrency have continued from the previous quarter.

We can know what the attackers are interested in, when we know the kind of attacks followed by the illegal access. Many cases of ransomware infection due to unauthorized login to the machines which could be remotely accessed from outside were reported earlier. However, recently the cases of cryptocurrency miner are being increasingly reported.

In order to understand the trends in cyber crime, if we look back from the perspective of attacks where “damage amount per incident is huge” and attacks where “number of incidents are large”, the cases where illegal remittance takes place from cryptocurrency exchange Coincheck are considered as attacks where “damage amount per incident is huge” and cases where there is an increase in the botnet that mines cryptocurrency are considered as attacks where “number of incidents are large”. The cryptocurrency is being attacked by various means and continued vigilance is required against these attacks. Previously, ransomware was used in attacks such as spamming e-mails where “number of incidents are large". However, recently ransomware attacks are carried out by aiming at specific targets followed by illegal intrusions. Thus the trend of ransomware attacks (SamSam etc.) is shifting towards attacks where "damage amount per incident is huge" demanding a large ransom.

Apart from cybercrime, the threat of WannaCry and its variants is increasing. In addition, attacks targeting the international event PyeongChang Olympics were also carried out. Besides that, CPU vulnerabilities were widely reported. This report further provides a timeline of security-related events that occurred in FY2017Q4. We have reflected on the relevance of events by summarizing the events into topics.

I. Hot Topic (1/6)

I-1. Prevalence of attacks targeting cryptocurrencies (Timeline [A, B, C])

Attackers are attempting to gain cryptocurrencies illegally using various means.

■ Classification of attacks targeting cryptocurrencies

Table 1 shows attacking techniques targeting cryptocurrencies classified by target. In the previous quarter's report (*1-1), this classification was used to consolidate data by comparing it against attacks targeting traditional currencies. In this report, we will consolidate the attacks reported in this quarter according to this classification.

Table 1: Classification of attacking techniques targeting cryptocurrencies

Classification	Target	Description and example of attack
Parties involved in cryptocurrency transactions	Cryptocurrency service providers	Attacks targeting Wallet of cryptocurrency exchange.
	Cryptocurrency service users	Attacks to steal authentication information used to login to the cryptocurrency exchange.
Regardless of cryptocurrency transactions	Computer owners	･Cryptocurrency miner ･Drive-by mining

■ Attacks targeting cryptocurrency service providers

Cryptocurrency NEM equivalent to 58 Billion Yen was illegally remitted from the cryptocurrency exchange Coincheck on January 26. It is assumed that **computers of multiple employees in the exchange who opened malicious mails were infected with malware** and the attacker remotely operated the computers and intruded into the network and stole the secret keys required for NEM transactions (*1-2). For attacks targeting cryptocurrency exchanges, countermeasures can be taken by both, the exchange and service users. In exchanges, it is valid to **manage secret keys offline or operate using multiple secret keys**. Service users can avoid damage by **moving funds from the wallet of the cryptocurrency exchange to the self-managed wallet after transactions**.

In the case where the Nepal bank SWIFT system was hacked and the amount was illegally remitted, they coordinated with the central bank to hold back the transaction and recovered major amount after noticing the illegal remittance (*1-3). On the other hand, stopping illegal remittance in cryptocurrency is a difficult and if community support is not forthcoming, the cryptocurrency may fork. In this case, it has been decided **not to take measures so as to undo the remittance because there was no problem with the mechanism of NEM** (*1-4).

As compared to traditional currency transactions, cryptocurrency transactions have advantages for attackers such as ease of creating cryptocurrency wallets or difficulty in recovering illegal remittance. While doing cryptocurrency transactions, it is required to be aware of such risks.

I. Hot Topic (2/6)

I-1. Prevalence of attacks targeting cryptocurrencies (Timeline [A, B, C])

■ Attacks targeting cryptocurrency service users

Users may be subjected to attacks not only while using the cryptocurrency services but also before using them.

- ✓ Attacks before using cryptocurrency services
  - ➢ Phishing mails were sent to the ICO (Initial Coin Offering) participants of Bee Token exchanged on the home sharing platform and about $1 Million was stolen (*1-5). According to the survey on cryptocurrencies in ICO, it has been reported that $400 million were stolen out of the $ 3.7 billion raised funds (* 1-6).
  - ➢ Cryptocurrency IOTA requires random alphanumeric characters 'seed' as a password for authentication. An attacker opened a site generating regular alphanumeric characters that mocked the site generating random alphanumeric characters used in 'seed'. It was easy for attacker to guess the password to access the created wallet using those alphanumeric characters and amount worth about $ 4 Million was stolen by the attacker (*1-7).
- ✓ Attacks while using cryptocurrency services
  - ➢ Wallet site manages the wallet required for cryptocurrency transactions on behalf of users. DNS server of the wallet site was hijacked, the address was redirected to the attacker's server, authentication information entered by the user was stolen and about $400,000 were stolen (*1-8).
  - ➢ Malwares Evrial (*1-9) and ComboJack (*1-10) were reported trying to steal the cryptocurrency by rewriting the cryptocurrency destination wallet address to the address of the attacker.

■ Attacks targeting computer owners

Cryptocurrency attacks target not only the parties involved in cryptocurrency transactions, but also the computer owners. Tendency to use all tricks to infect the miner and to do drive-by mining has become prominent. They are summarized in Timeline [C] on P.14. Moreover, many botnets that mine cryptocurrencies were also reported. They are summarized in Table 2.

Table 2: Cryptocurrency mining botnets

Name of Botnet	Description
PyCryptoMiner (*1-11)	Written in Python. Targets almost all Linux/Windows.
WannaMine (*1-12)	Spreads using EternalBlue.
DDG.Mining (*1-13)	Spreads using OrientDB vulnerabilities.
ADB.miner (*1-14)	Spreads by targeting debug ports of Android devices.
Smominru (*1-15)	Spreads using EternalBlue and EsteemAudit. It is also reported as MyKings (*1-16).

I. Hot Topic (3/6)

I-2. Continued threats of WannaCry and its variants (Timeline [E])

Vulnerability targeted by WannaCry is constantly attacked.

■ Prevalence of attacks targeting vulnerability of file sharing service

The vulnerability targeted by WannaCry which was prevalent worldwide in May 2017 continues to be targeted even now. Figure 1 shows the number of IP addresses used for conducting activities that targeted the vulnerability. From Figure 1, **we can see the activities of malware other than WannaCry and its variants targeting the vulnerability before prevalence of WannaCry in May and around December**. Moreover, we can see that **the number of machines infected with WannaCry and its variants are continuously increasing**.

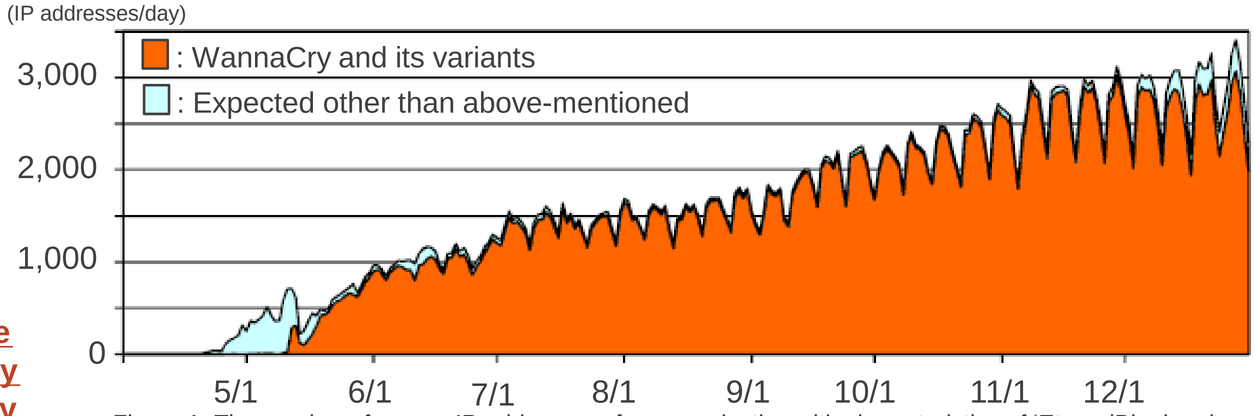


Figure 1: The number of source IP addresses of communication with characteristics of ‘EternalBlue’ and ‘DoublePulsar’ scan tools (Quoted from ‘Police Agency @ police: Internet Observation Results (Y2017) (* 1-17)’)

EternalBlue: Attack tool which executes code remotely for the vulnerability of Windows file sharing service.

DoublePulsar: Back door that infects Windows. It can infect using the above-mentioned EternalBlue. DoublePulsar is also installed at the time of WannaCry infection.

■ Communication targeting the vulnerability increased from around December

It was reported that there were tens of thousands of machines infected with DoublePulsar due to the vulnerability before the worldwide prevalence of WannaCry in May 2017 (*1-18). This must have been associated with the communication observed from April to early May. From December onwards, malwares other than WannaCry and its variants are observed to be attacking the vulnerability again. **It may be the communication from the cryptocurrency mining bot that spreads infection targeting the vulnerability** (*1-12,1-15). Moreover, **it may also be trying to attack via DoublePulsar targeting the machines infected with WannaCry variants**. **Vulnerabilities that are easy to exploit for attackers will be constantly targeted for a long time.** It is required to cope with this in a convincing way.

I. Hot Topic (4/6)

I-2. Continued threats of WannaCry and its variants (Timeline [E])

■ Prevalence of WannaCry variants

The WannaCry variant has the features such that the **infectious activities are carried out regardless the kill switch connection, files are not encrypted and ransom notes are not displayed** (*1-17). Since June 2017, infection has been reported at least in the following organizations.

➢ June	"McDonald's Company (Japan), Ltd." (*1-19)
➢ October	Medical Institutions Group "FirstHealth of the Carolinas, Inc." in the US (*1-20)
➢ January	"NTT DATA Corporation" in Japan (*1-21)
➢ March	"The Boeing Company" in the US (*1-22)

It is observed that there is increase in the number of machines infected with WannaCry and its variants. This may be because some machines are potentially left without patches. We have considered the cases that require attention, in the environments where patches have not been applied.

✓ Bringing machines into a closed NW

Let us consider the case where machines with vulnerabilities left on them are allowed in a closed NW without having internet connectivity. In such environments, it is required to pay special attention to the machines brought in from outside. It is considered that the rules for the machines to be brought in are strictly stipulated and followed, however, **assuming that the machine may be brought in by bypassing the rules for some reason**, some measures need to be taken by the system such as deploying the quarantine NW.

✓ Thin client terminal

Writing to the hard disks of thin client terminals is often restricted and it is assumed that it is difficult to apply patches after purchasing the terminals. **Since WannaCry variants operate on memory and spread infection, it is spread even if writing on hard disk is restricted**. It is also required to **apply the patches to the thin client terminals from the management tools or remotely**.

I. Hot Topic (5/6)

I-3. Other Topics

- **From early January, CPU vulnerabilities (Meltdown, Spectre) became a hot topic (Timeline [G]).**
  - ✓ The speculative execution was abused and most of the CPUs (*1-23, 1-24, 1-25) distributed in the market were affected.
  - ✓ **Attacker is required to run malicious code on the target system for exploiting this vulnerability**. Following 2 possible attack scenarios are of concern.
    - ➢ Steal data on the memory of another guest OS (another customer) in the cloud environment.
    - ➢ Steal data (authentication information and cookies) of another site using JavaScript in a Web browser.

    For these reasons, cloud service providers and web browser developers were forced to respond to vulnerabilities.
  - ✓ Depending on the nature of the system, there is a **risk of performance degradation due to the application of patches** (*1-26). Adequate verification is required for patch application.

- **A DDoS attack on GitHub using memcached UDP reflection vulnerability (CVE - 2018 - 1000115) (Timeline [H]).**
  - ✓ **Memcached servers exposed to the public internet* were abused for attacks**. In the survey using online search engine ‘Shodan’, about 10,000 servers were exposed worldwide as of March 3 (*1-27).
  - ✓ **The size of the DDoS attack on GitHub has reached to 1.3 Tbps, the largest in the past**. The communication source was distributed over thousand or more AS and tens of thousands of source IPs and the amplification rate of UDP reflection was about 50,000 times (*1-28).
  - ✓ **Leaving the vulnerability unattended not only makes it a victim of cyber attack, but there are cases where it becomes a perpetrator unknowingly**. It is important to manage the configuration of the software and version used by your organization, collect and handle the vulnerability information appropriately.

* Memcached is an on-memory cache server used to speed up web applications.
It is not required to expose it to the public internet in general applications.

I. Hot Topic (6/6)

I-3. Other Topics

- **Cyber attack in PyeongChang Olympics (Timeline[I]).**
  - ✓ There was **cyber attack through e-mail targeting the Olympic stakeholders before opening in December 2017** (*1-29).
  - ✓ There was **cyber attack on the day of opening ceremony on February 9th that led to problems in few services** (*1-30).
    - ➢ The official Olympics website went down
    - ➢ The televisions and internet in the main press center stopped working
    - ➢ The Wi-Fi in the PyeongChang Olympic stadium also stopped working
  - ✓ **In international event, the cyber attacks (also including reconnaissance or hiding) occur before the opening of event with the purpose of money, demonstration, blackmail etc.** Sufficient security measures against the important infrastructure and ability to recover (resilience) from intrusion or attack are needed.

- **Continued instances of attack on supply chains (Timeline [J]).**
  - ✓ Attack targeting software developers
    - ➢ **Adware was installed in Android SDK** in China. Advertisements were displayed when the application developed using SDK was installed(*1-31).
    - ➢ **The download link of the official site** of software phpBB for creating bulletin board **was rewrote** and used in malware distribution (*1-32).
  - ✓ Attack targeting goods sellers
    - ➢ **Budget Android smartphones with pre-installed banking Trojan Triada** were sold in China (*1-33).

II. Forecast
II-1. Cryptocurrency mining function is added to banking Trojan and ransomware

- **The creators of banking Trojan wanted to reap a lot of benefits using malware**

LokiBot is reported as a malware that combines the functions of banking Trojan and ransomware (*2-1). LokiBot is usually concealed in the infected device, and steals the information. However, when it is noticed and tried to remove from the infected device, it encrypts the files in the device and locks the screen.

The attackers might lock the screen immediately after infecting the device and demand a ransom. However, **they try to reap maximum benefit by one infection** combining several methods until the malware activities are revealed.

- **Coexistence of cryptocurrency mining function, banking Trojan and ransomware**

The cryptocurrency miners steal the computing resources from the infected device and mine the cryptocurrency. The attackers do not want the user to notice the infection as long as possible so that they can mine the cryptocurrency during that period. There are also miners limiting CPU usage (*2-2).

Both cryptocurrency miners and banking Trojan cause malware infection that is unlikely to be noticed. **Besides stealing and hiding the information, banking Trojan may mine the cryptocurrency secretly.**

If cryptocurrency mining and ransomware are compared, cryptocurrency miners do not want to get the infection to be noticed, on the contrary, ransomware needs the infection to be noticed. However, like the above-mentioned LokiBot, **it may coexist with the ransomware that attacks after being noticed**.

NTTDATA-CERT is concerned that such **cryptocurrency mining features will be added in banking Trojan or ransomware.** For example, the information is stolen and cryptocurrency mining is carried out before anyone can notice, and even if it gets noticed, the malware will encrypt the files in the device.

II. Forecast

II-2. Cryptocurrency miners aim at coexistence with computer owners

■ The difference between cryptocurrency miners and other malware

The cryptocurrency miners steal the computing resources from the infected device and mine the cryptocurrency. The banking Trojan or ransomware explicitly compromise the Confidentiality, Integrity and Availability of users. On the other hand, cryptocurrency miners may affect ‘Availability’ by consuming computing resource. However, the ‘Availability’ may not be compromised by fixing the computing resources. For a user, the damage is theft of computing resources. However, depending on the conditions, the damage may not be unacceptable to the user. NTTDATA-CERT is concerned that **cryptocurrency miners aim at coexistence with computer owners**.

■ Forecast (1): Offer exchange conditions for cryptocurrency mining to the users and mine cryptocurrency on obtaining their consent.

Since the user agrees, it may not be called as malware. However, the cryptocurrency miners **mining the cryptocurrency by offering exchange conditions** might go on increasing. Many cases have already reported for software demanding cryptocurrency mining with exchange conditions using functions. Also, there are examples of deletion from official app store that leaves a bad impact on the user (*2-3,2-4).

Cryptocurrency miners that stop the activities of other miners and try to occupy computing resources were found (*2-5). The exchange conditions offered by attackers have not only the usage rights of software as mentioned above but also conditions **to monitor so that other miners or malware will not be active**.

■ Forecast (2): Mining according to the active/inactive status of computer owners.

The cryptocurrency miners that coexist secretly may emerge eliminating as far as possible, the possibility of being noticed by the users. They monitor the usage status of computing resource and **carry out mining targeting the time zone when computing resources are not in use**. For example, if the computers in office are to be infected, they may be active only during the lunchtime.

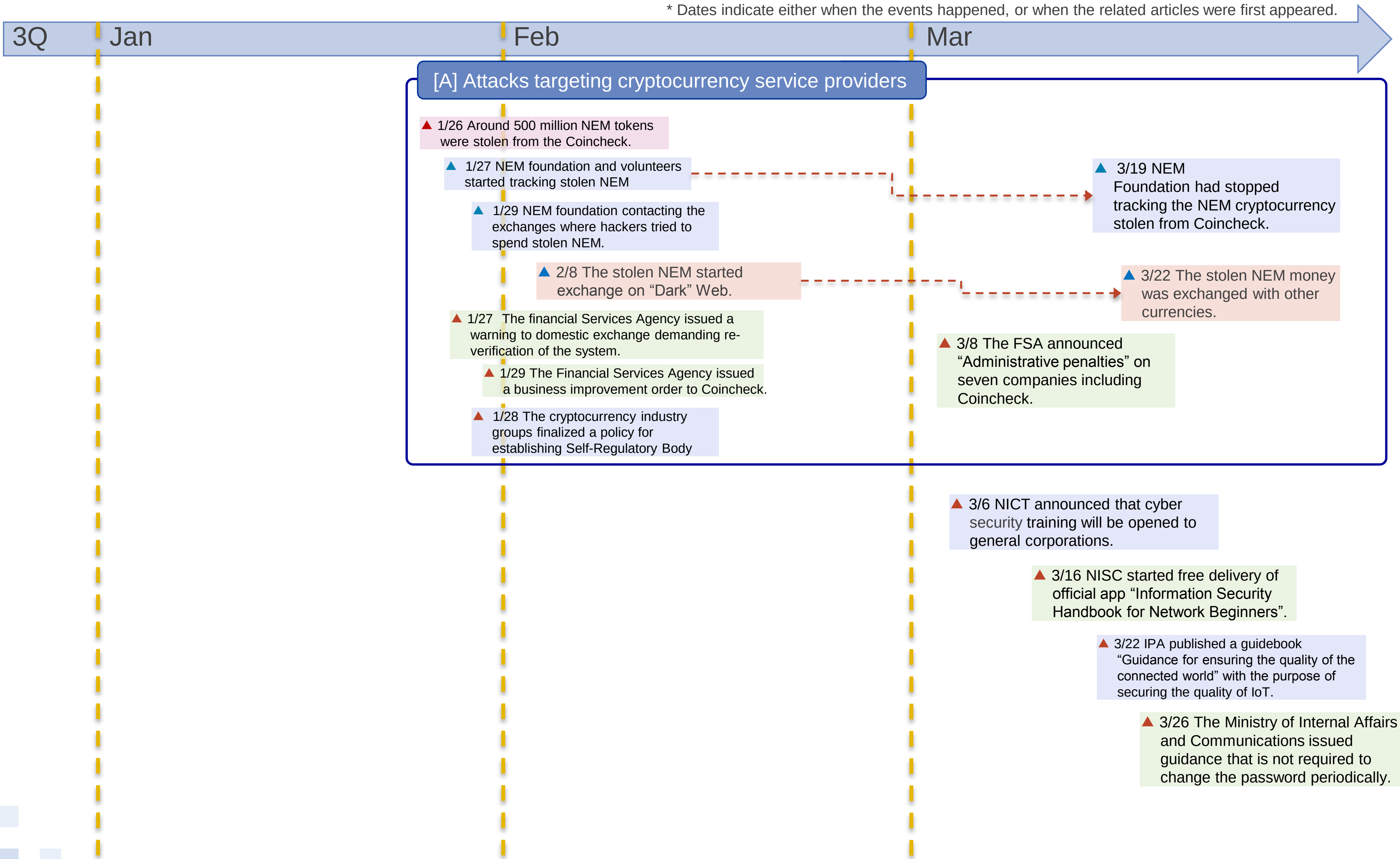
III. Timeline (1/9)

▲: 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] Attacks targeting cryptocurrency service providers

▲ 1/26 Around 500 million NEM tokens were stolen from the Coincheck.

▲ 1/27 NEM foundation and volunteers started tracking stolen NEM

▲ 1/29 NEM foundation contacting the exchanges where hackers tried to spend stolen NEM.

▲ 2/8 The stolen NEM started exchange on “Dark” Web.

▲ 1/27 The financial Services Agency issued a warning to domestic exchange demanding re-verification of the system.

▲ 1/29 The Financial Services Agency issued a business improvement order to Coincheck.

▲ 1/28 The cryptocurrency industry groups finalized a policy for establishing Self-Regulatory Body

▲ 3/19 NEM Foundation had stopped tracking the NEM cryptocurrency stolen from Coincheck.

▲ 3/22 The stolen NEM money was exchanged with other currencies.

▲ 3/8 The FSA announced “Administrative penalties” on seven companies including Coincheck.

▲ 3/6 NICT announced that cyber security training will be opened to general corporations.

▲ 3/16 NISC started free delivery of official app “Information Security Handbook for Network Beginners”.

▲ 3/22 IPA published a guidebook “Guidance for ensuring the quality of the connected world” with the purpose of securing the quality of IoT.

▲ 3/26 The Ministry of Internal Affairs and Communications issued guidance that is not required to change the password periodically.

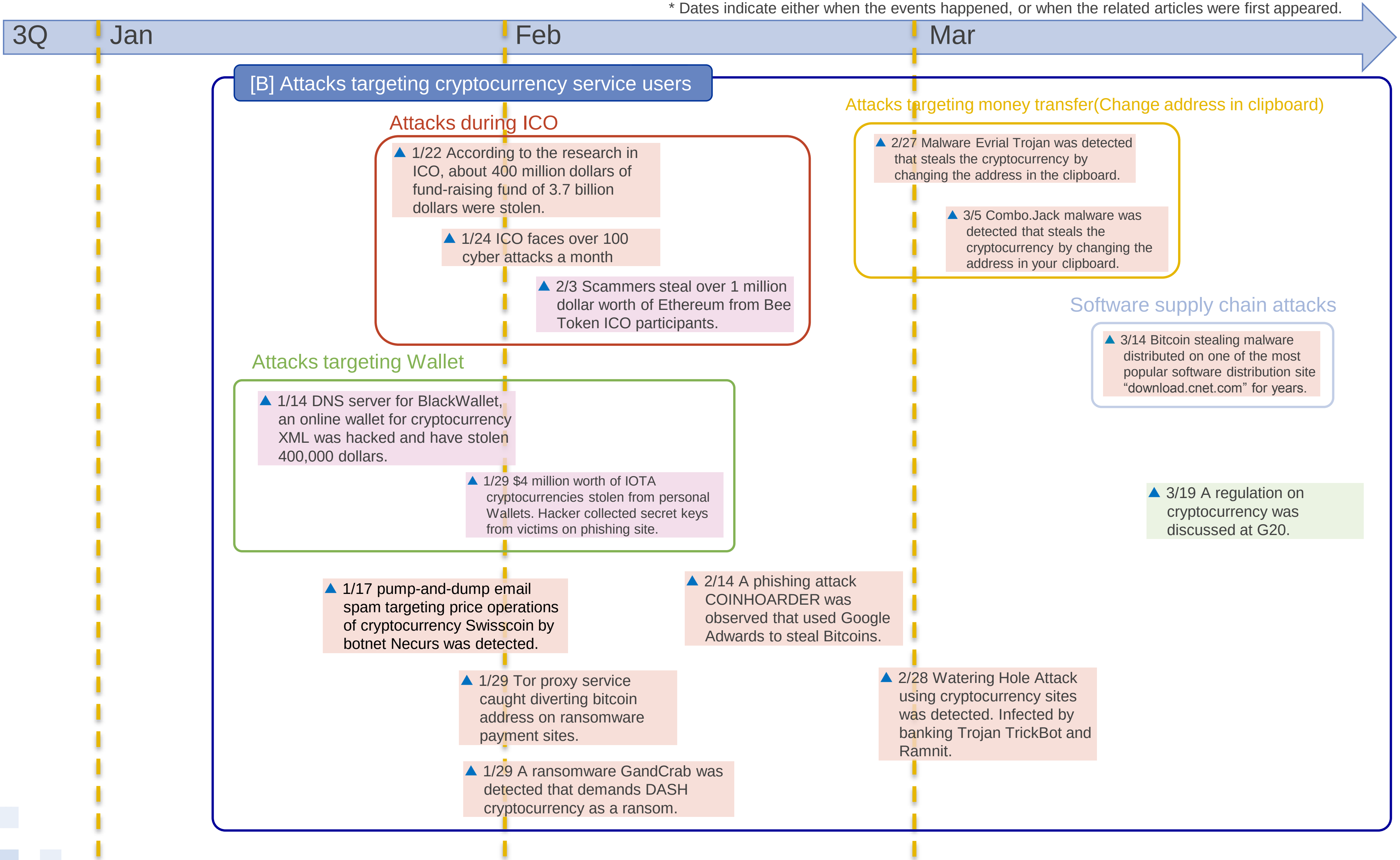
III. Timeline (2/9)

▲: 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 cryptocurrency service users

Attacks during ICO

▲ 1/22 According to the research in ICO, about 400 million dollars of fund-raising fund of 3.7 billion dollars were stolen.

▲ 1/24 ICO faces over 100 cyber attacks a month

▲ 2/3 Scammers steal over 1 million dollar worth of Ethereum from Bee Token ICO participants.

Attacks targeting Wallet

▲ 1/14 DNS server for BlackWallet, an online wallet for cryptocurrency XML was hacked and have stolen 400,000 dollars.

▲ 1/29 $4 million worth of IOTA cryptocurrencies stolen from personal Wallets. Hacker collected secret keys from victims on phishing site.

▲ 1/17 pump-and-dump email spam targeting price operations of cryptocurrency Swisscoin by botnet Necurs was detected.

▲ 1/29 Tor proxy service caught diverting bitcoin address on ransomware payment sites.

▲ 1/29 A ransomware GandCrab was detected that demands DASH cryptocurrency as a ransom.

▲ 2/14 A phishing attack COINHOARDER was observed that used Google Adwards to steal Bitcoins.

Attacks targeting money transfer(Change address in clipboard)

▲ 2/27 Malware Evrial Trojan was detected that steals the cryptocurrency by changing the address in the clipboard.

▲ 3/5 Combo.Jack malware was detected that steals the cryptocurrency by changing the address in your clipboard.

▲ 2/28 Watering Hole Attack using cryptocurrency sites was detected. Infected by banking Trojan TrickBot and Ramnit.

Software supply chain attacks

▲ 3/14 Bitcoin stealing malware distributed on one of the most popular software distribution site “download.cnet.com” for years.

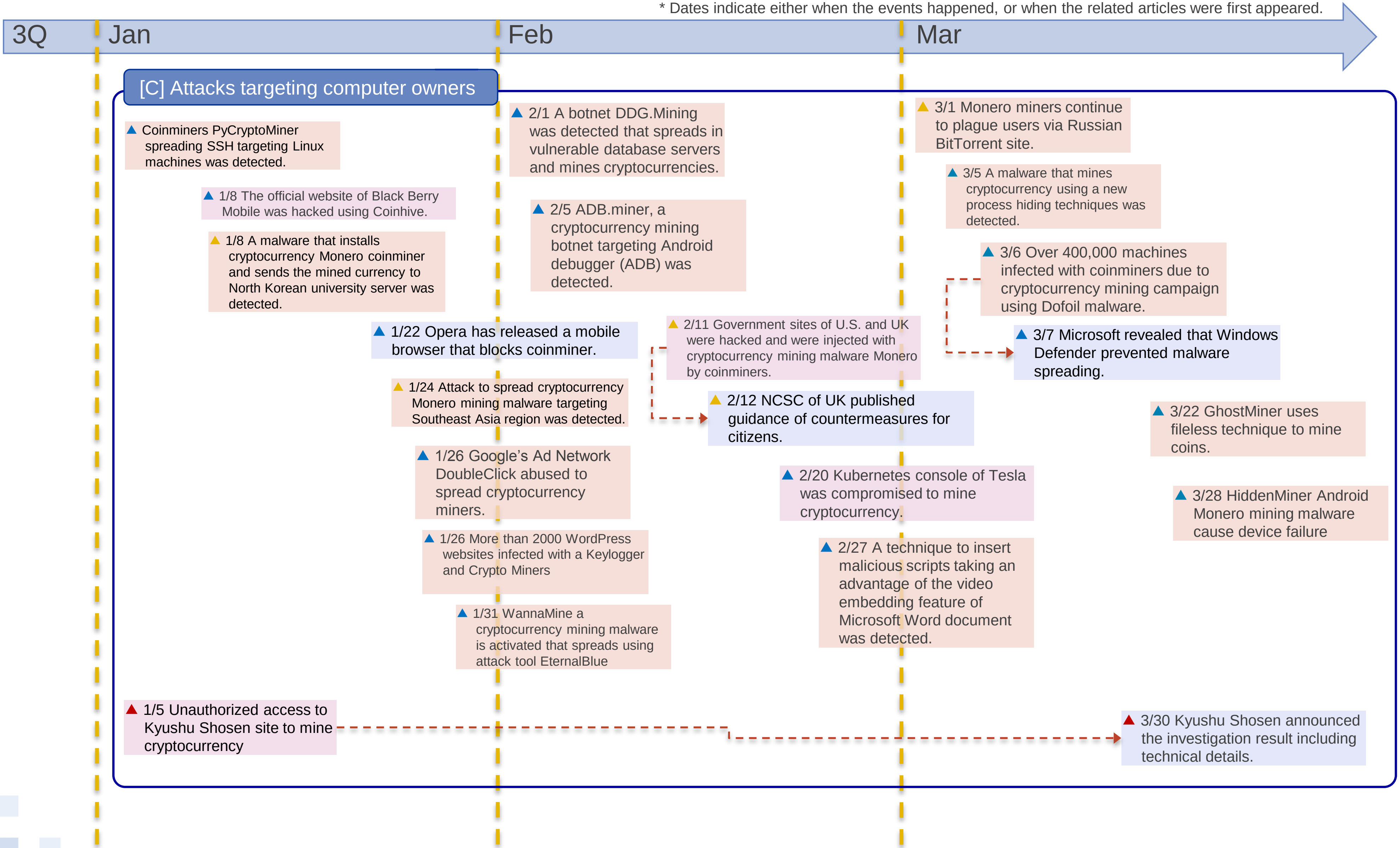
▲ 3/19 A regulation on cryptocurrency was discussed at G20.

III. Timeline (3/9)

▲: 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.

3Q | Jan | Feb | Mar

[C] Attacks targeting computer owners

▲ Coinminers PyCryptoMiner spreading SSH targeting Linux machines was detected.

▲ 1/8 The official website of Black Berry Mobile was hacked using Coinhive.

▲ 1/8 A malware that installs cryptocurrency Monero coinminer and sends the mined currency to North Korean university server was detected.

▲ 1/22 Opera has released a mobile browser that blocks coinminer.

▲ 1/24 Attack to spread cryptocurrency Monero mining malware targeting Southeast Asia region was detected.

▲ 1/26 Google's Ad Network DoubleClick abused to spread cryptocurrency miners.

▲ 1/26 More than 2000 WordPress websites infected with a Keylogger and Crypto Miners

▲ 1/31 WannaMine a cryptocurrency mining malware is activated that spreads using attack tool EternalBlue

▲ 1/5 Unauthorized access to Kyushu Shosen site to mine cryptocurrency

▲ 2/1 A botnet DDG.Mining was detected that spreads in vulnerable database servers and mines cryptocurrencies.

▲ 2/5 ADB.miner, a cryptocurrency mining botnet targeting Android debugger (ADB) was detected.

▲ 2/11 Government sites of U.S. and UK were hacked and were injected with cryptocurrency mining malware Monero by coinminers.

▲ 2/12 NCSC of UK published guidance of countermeasures for citizens.

▲ 2/20 Kubernetes console of Tesla was compromised to mine cryptocurrency.

▲ 2/27 A technique to insert malicious scripts taking an advantage of the video embedding feature of Microsoft Word document was detected.

▲ 3/1 Monero miners continue to plague users via Russian BitTorrent site.

▲ 3/5 A malware that mines cryptocurrency using a new process hiding techniques was detected.

▲ 3/6 Over 400,000 machines infected with coinminers due to cryptocurrency mining campaign using Dofoil malware.

▲ 3/7 Microsoft revealed that Windows Defender prevented malware spreading.

▲ 3/22 GhostMiner uses fileless technique to mine coins.

▲ 3/28 HiddenMiner Android Monero mining malware cause device failure

▲ 3/30 Kyushu Shosen announced the investigation result including technical details.

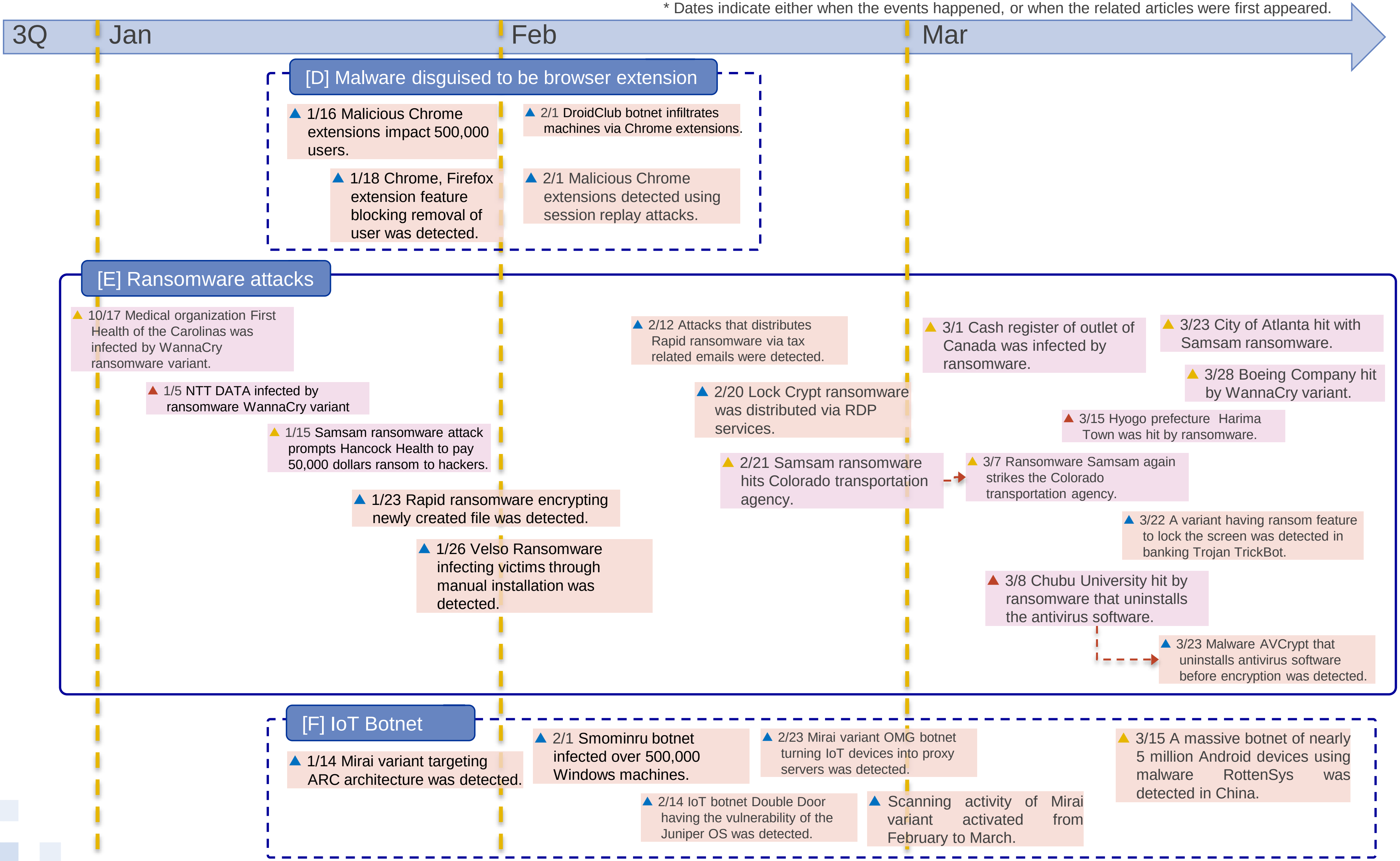
III. Timeline (4/9)

▲: 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.



[D] Malware disguised to be browser extension

- ▲ 1/16 Malicious Chrome extensions impact 500,000 users.
- ▲ 1/18 Chrome, Firefox extension feature blocking removal of user was detected.
- ▲ 2/1 DroidClub botnet infiltrates machines via Chrome extensions.
- ▲ 2/1 Malicious Chrome extensions detected using session replay attacks.

[E] Ransomware attacks

- ▲ 10/17 Medical organization First Health of the Carolinas was infected by WannaCry ransomware variant.
- ▲ 1/5 NTT DATA infected by ransomware WannaCry variant
- ▲ 1/15 Samsam ransomware attack prompts Hancock Health to pay 50,000 dollars ransom to hackers.
- ▲ 1/23 Rapid ransomware encrypting newly created file was detected.
- ▲ 1/26 Velso Ransomware infecting victims through manual installation was detected.
- ▲ 2/12 Attacks that distributes Rapid ransomware via tax related emails were detected.
- ▲ 2/20 Lock Crypt ransomware was distributed via RDP services.
- ▲ 2/21 Samsam ransomware hits Colorado transportation agency.
- ▲ 3/7 Ransomware Samsam again strikes the Colorado transportation agency.
- ▲ 3/1 Cash register of outlet of Canada was infected by ransomware.
- ▲ 3/23 City of Atlanta hit with Samsam ransomware.
- ▲ 3/28 Boeing Company hit by WannaCry variant.
- ▲ 3/15 Hyogo prefecture Harima Town was hit by ransomware.
- ▲ 3/22 A variant having ransom feature to lock the screen was detected in banking Trojan TrickBot.
- ▲ 3/8 Chubu University hit by ransomware that uninstalls the antivirus software.
- ▲ 3/23 Malware AVCrypt that uninstalls antivirus software before encryption was detected.

[F] IoT Botnet

- ▲ 1/14 Mirai variant targeting ARC architecture was detected.
- ▲ 2/1 Smominru botnet infected over 500,000 Windows machines.
- ▲ 2/14 IoT botnet Double Door having the vulnerability of the Juniper OS was detected.
- ▲ 2/23 Mirai variant OMG botnet turning IoT devices into proxy servers was detected.
- ▲ Scanning activity of Mirai variant activated from February to March.
- ▲ 3/15 A massive botnet of nearly 5 million Android devices using malware RottenSys was detected in China.

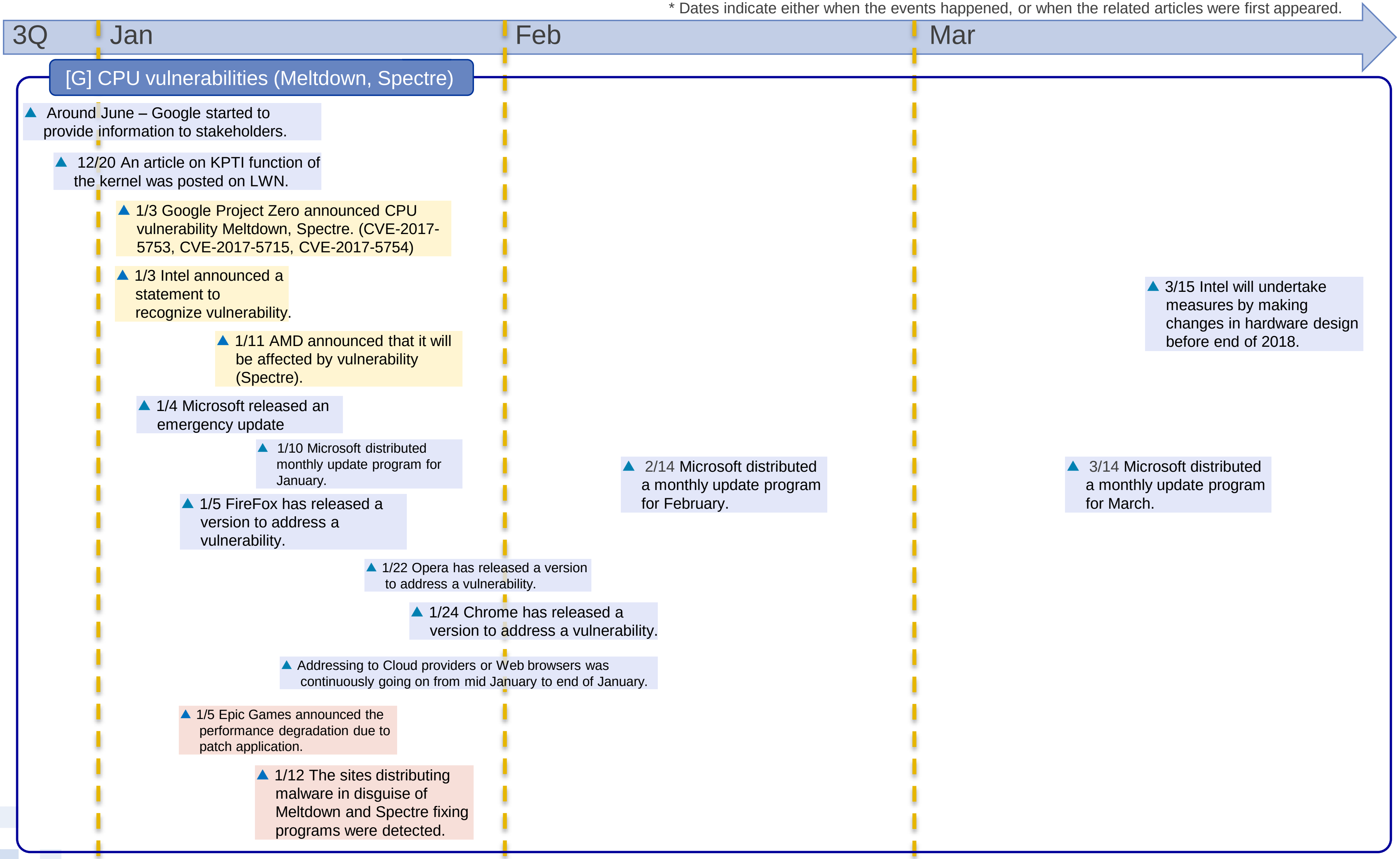
III. Timeline (5/9)

▲: 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.



[G] CPU vulnerabilities (Meltdown, Spectre)

▲ Around June – Google started to provide information to stakeholders.

▲ 12/20 An article on KPTI function of the kernel was posted on LWN.

▲ 1/3 Google Project Zero announced CPU vulnerability Meltdown, Spectre. (CVE-2017-5753, CVE-2017-5715, CVE-2017-5754)

▲ 1/3 Intel announced a statement to recognize vulnerability.

▲ 1/11 AMD announced that it will be affected by vulnerability (Spectre).

▲ 1/4 Microsoft released an emergency update

▲ 1/10 Microsoft distributed monthly update program for January.

▲ 1/5 FireFox has released a version to address a vulnerability.

▲ 1/22 Opera has released a version to address a vulnerability.

▲ 1/24 Chrome has released a version to address a vulnerability.

▲ Addressing to Cloud providers or Web browsers was continuously going on from mid January to end of January.

▲ 1/5 Epic Games announced the performance degradation due to patch application.

▲ 1/12 The sites distributing malware in disguise of Meltdown and Spectre fixing programs were detected.

▲ 2/14 Microsoft distributed a monthly update program for February.

▲ 3/15 Intel will undertake measures by making changes in hardware design before end of 2018.

▲ 3/14 Microsoft distributed a monthly update program for March.

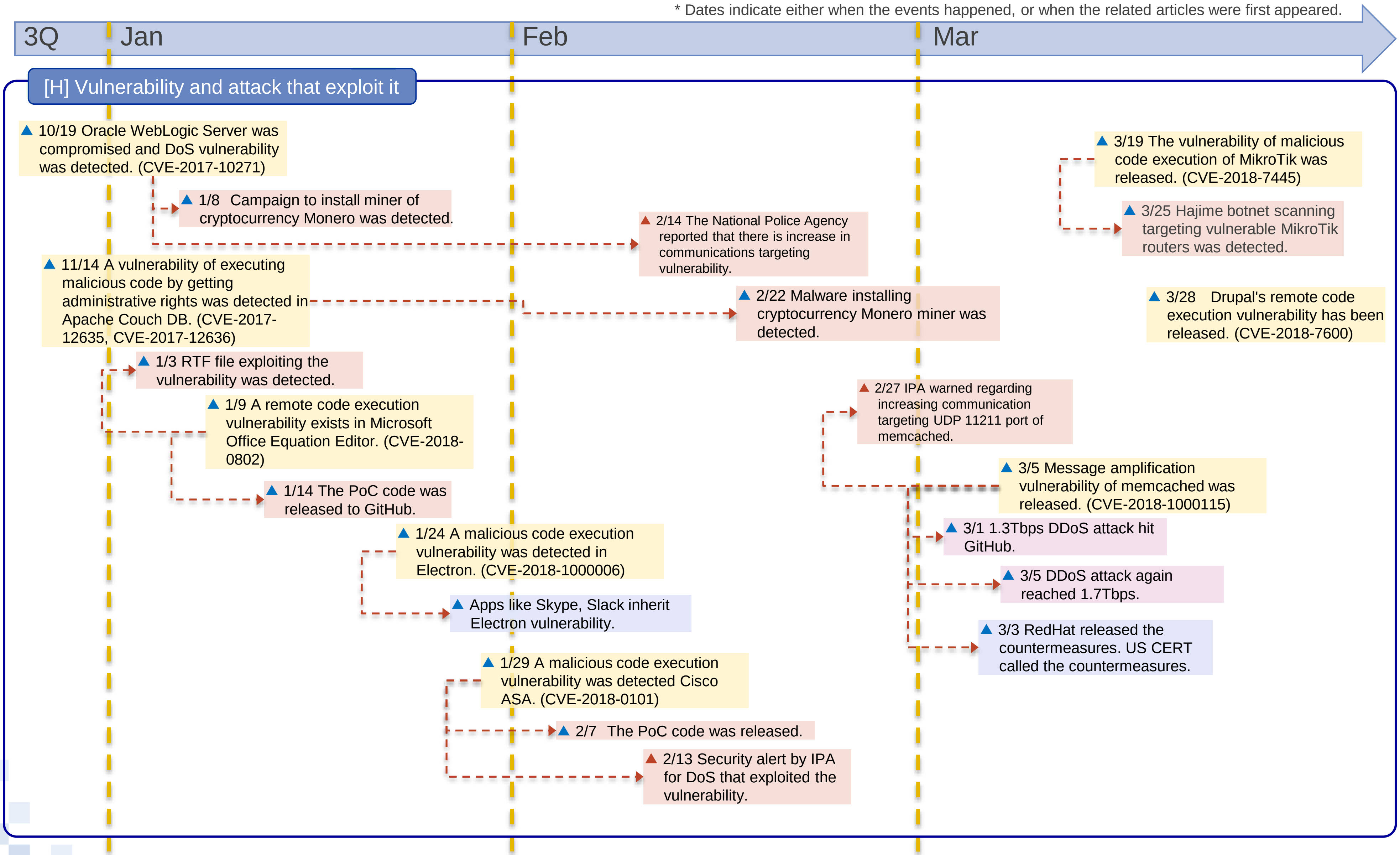
III. Timeline (6/9)

▲: 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.



[H] Vulnerability and attack that exploit it

▲ 10/19 Oracle WebLogic Server was compromised and DoS vulnerability was detected. (CVE-2017-10271)

▲ 1/8 Campaign to install miner of cryptocurrency Monero was detected.

▲ 2/14 The National Police Agency reported that there is increase in communications targeting vulnerability.

▲ 11/14 A vulnerability of executing malicious code by getting administrative rights was detected in Apache Couch DB. (CVE-2017-12635, CVE-2017-12636)

▲ 2/22 Malware installing cryptocurrency Monero miner was detected.

▲ 1/3 RTF file exploiting the vulnerability was detected.

▲ 1/9 A remote code execution vulnerability exists in Microsoft Office Equation Editor. (CVE-2018-0802)

▲ 1/14 The PoC code was released to GitHub.

▲ 1/24 A malicious code execution vulnerability was detected in Electron. (CVE-2018-1000006)

▲ Apps like Skype, Slack inherit Electron vulnerability.

▲ 1/29 A malicious code execution vulnerability was detected Cisco ASA. (CVE-2018-0101)

▲ 2/7 The PoC code was released.

▲ 2/13 Security alert by IPA for DoS that exploited the vulnerability.

▲ 2/27 IPA warned regarding increasing communication targeting UDP 11211 port of memcached.

▲ 3/5 Message amplification vulnerability of memcached was released. (CVE-2018-1000115)

▲ 3/1 1.3Tbps DDoS attack hit GitHub.

▲ 3/5 DDoS attack again reached 1.7Tbps.

▲ 3/3 RedHat released the countermeasures. US CERT called the countermeasures.

▲ 3/19 The vulnerability of malicious code execution of MikroTik was released. (CVE-2018-7445)

▲ 3/25 Hajime botnet scanning targeting vulnerable MikroTik routers was detected.

▲ 3/28 Drupal's remote code execution vulnerability has been released. (CVE-2018-7600)

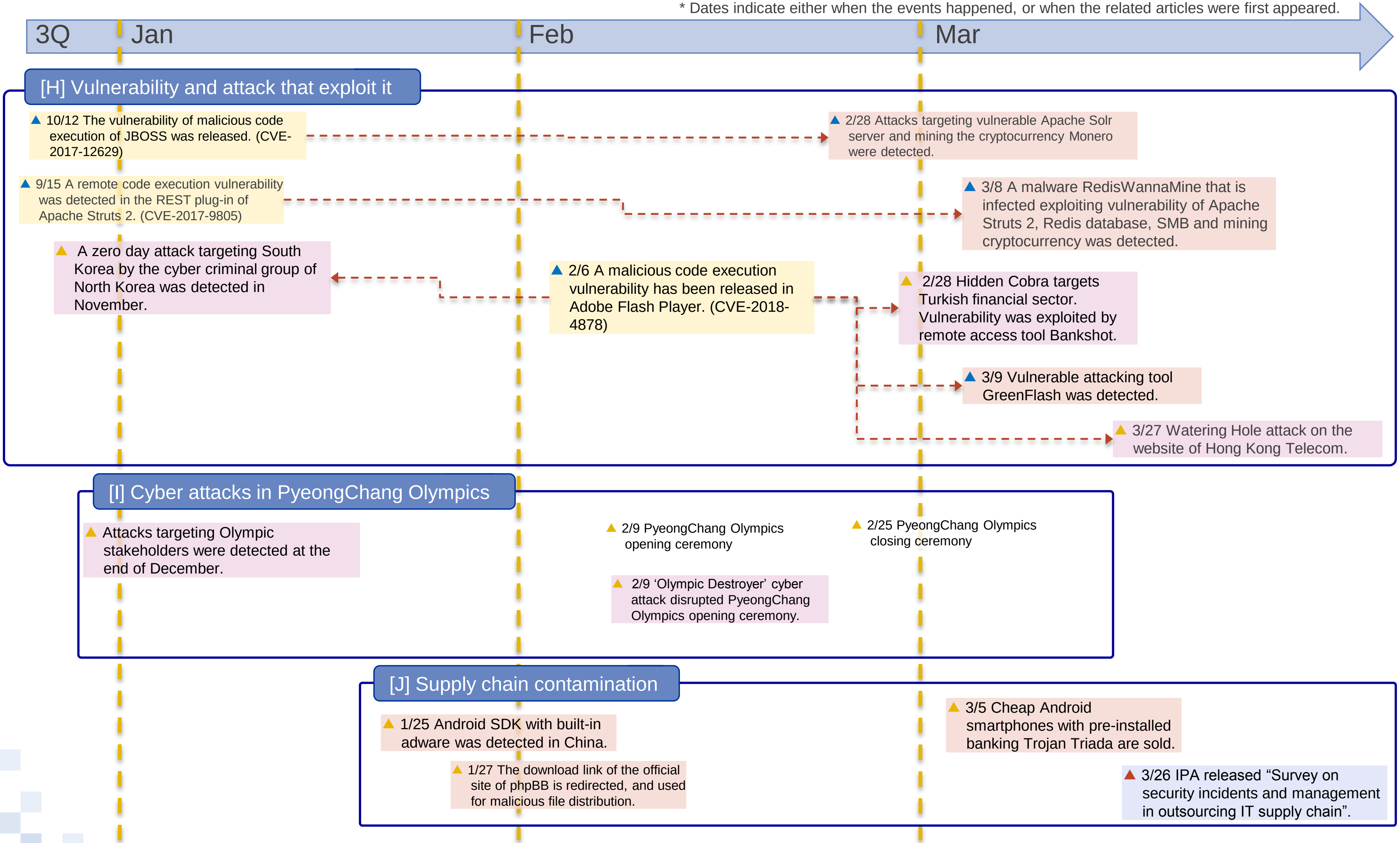
III. Timeline (7/9)

▲: 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.



3Q | Jan | Feb | Mar

[H] Vulnerability and attack that exploit it

▲ 10/12 The vulnerability of malicious code execution of JBOSS was released. (CVE-2017-12629)

▲ 2/28 Attacks targeting vulnerable Apache Solr server and mining the cryptocurrency Monero were detected.

▲ 9/15 A remote code execution vulnerability was detected in the REST plug-in of Apache Struts 2. (CVE-2017-9805)

▲ 3/8 A malware RedisWannaMine that is infected exploiting vulnerability of Apache Struts 2, Redis database, SMB and mining cryptocurrency was detected.

▲ A zero day attack targeting South Korea by the cyber criminal group of North Korea was detected in November.

▲ 2/6 A malicious code execution vulnerability has been released in Adobe Flash Player. (CVE-2018-4878)

▲ 2/28 Hidden Cobra targets Turkish financial sector. Vulnerability was exploited by remote access tool Bankshot.

▲ 3/9 Vulnerable attacking tool GreenFlash was detected.

▲ 3/27 Watering Hole attack on the website of Hong Kong Telecom.

[I] Cyber attacks in PyeongChang Olympics

▲ Attacks targeting Olympic stakeholders were detected at the end of December.

▲ 2/9 PyeongChang Olympics opening ceremony

▲ 2/25 PyeongChang Olympics closing ceremony

▲ 2/9 ‘Olympic Destroyer’ cyber attack disrupted PyeongChang Olympics opening ceremony.

[J] Supply chain contamination

▲ 1/25 Android SDK with built-in adware was detected in China.

▲ 1/27 The download link of the official site of phpBB is redirected, and used for malicious file distribution.

▲ 3/5 Cheap Android smartphones with pre-installed banking Trojan Triada are sold.

▲ 3/26 IPA released “Survey on security incidents and management in outsourcing IT supply chain”.

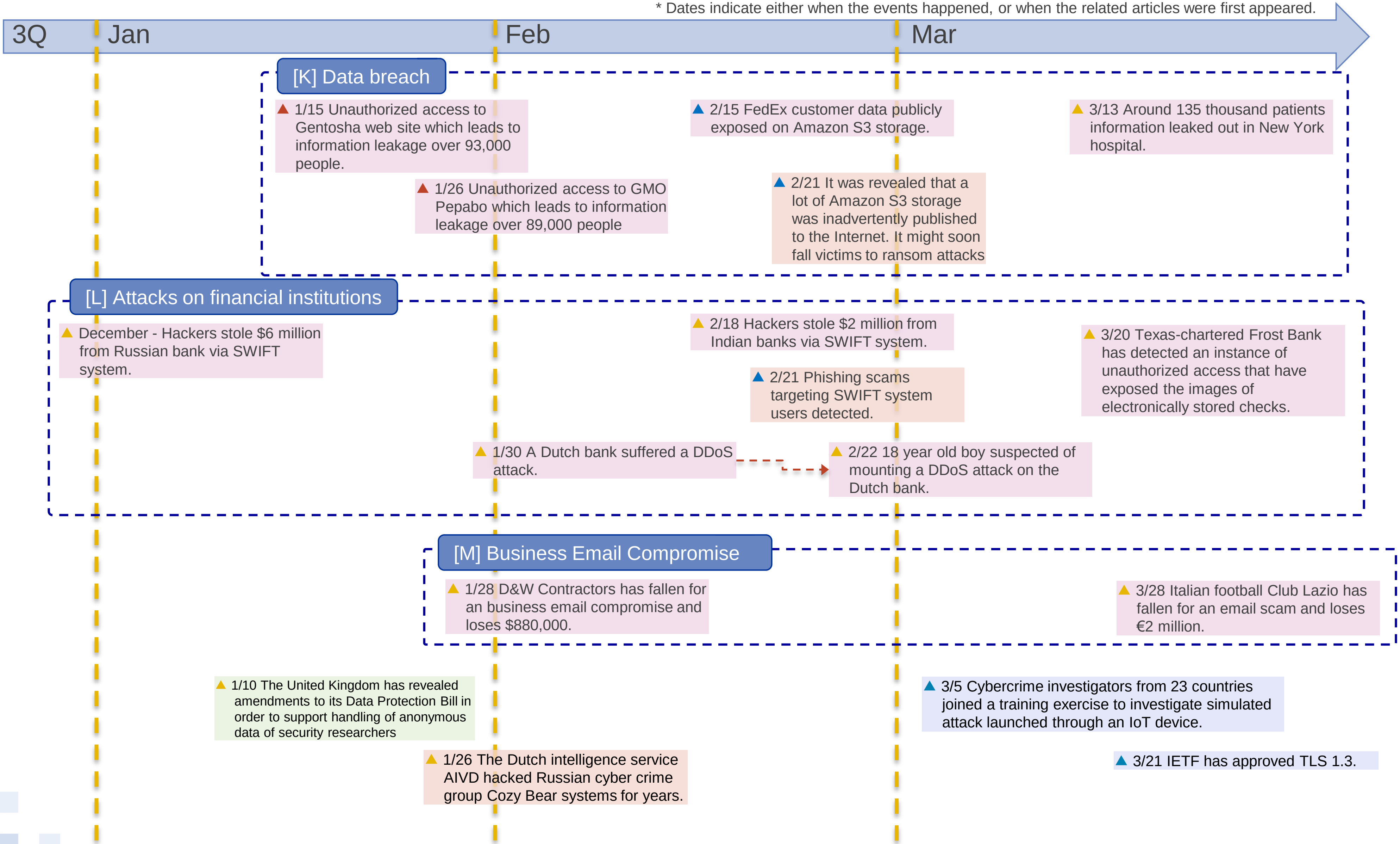
III. Timeline (8/9)

▲: 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.



[K] Data breach

▲ 1/15 Unauthorized access to Gentosha web site which leads to information leakage over 93,000 people.

▲ 1/26 Unauthorized access to GMO Pepabo which leads to information leakage over 89,000 people

▲ 2/15 FedEx customer data publicly exposed on Amazon S3 storage.

▲ 2/21 It was revealed that a lot of Amazon S3 storage was inadvertently published to the Internet. It might soon fall victims to ransom attacks

▲ 3/13 Around 135 thousand patients information leaked out in New York hospital.

[L] Attacks on financial institutions

▲ December - Hackers stole $6 million from Russian bank via SWIFT system.

▲ 1/30 A Dutch bank suffered a DDoS attack.

▲ 2/18 Hackers stole $2 million from Indian banks via SWIFT system.

▲ 2/21 Phishing scams targeting SWIFT system users detected.

▲ 2/22 18 year old boy suspected of mounting a DDoS attack on the Dutch bank.

▲ 3/20 Texas-chartered Frost Bank has detected an instance of unauthorized access that have exposed the images of electronically stored checks.

[M] Business Email Compromise

▲ 1/28 D&W Contractors has fallen for an business email compromise and loses $880,000.

▲ 3/28 Italian football Club Lazio has fallen for an email scam and loses €2 million.

▲ 1/10 The United Kingdom has revealed amendments to its Data Protection Bill in order to support handling of anonymous data of security researchers

▲ 1/26 The Dutch intelligence service AIVD hacked Russian cyber crime group Cozy Bear systems for years.

▲ 3/5 Cybercrime investigators from 23 countries joined a training exercise to investigate simulated attack launched through an IoT device.

▲ 3/21 IETF has approved TLS 1.3.

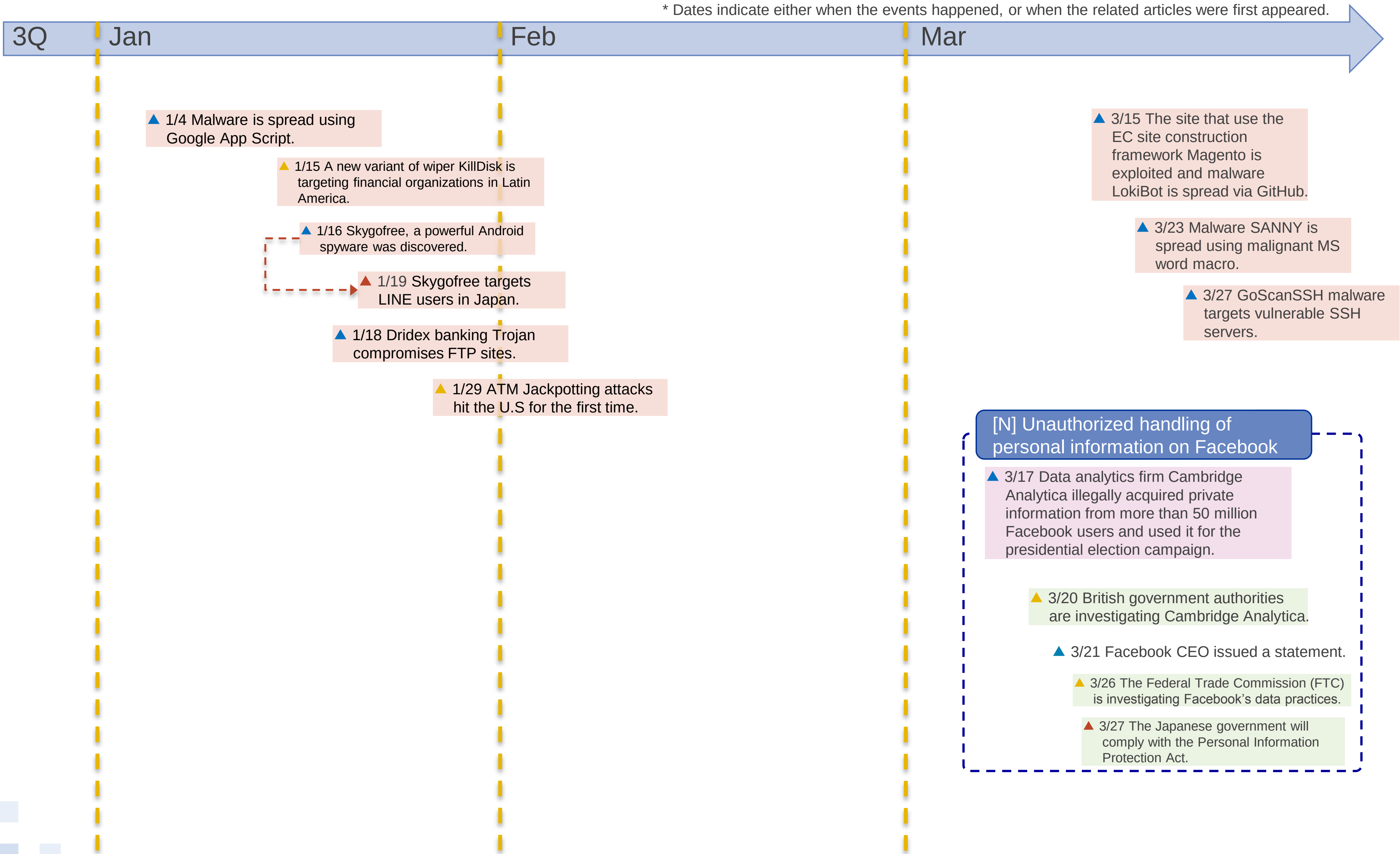
III. Timeline (9/9)

▲: 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.



▲ 1/4 Malware is spread using Google App Script.

▲ 1/15 A new variant of wiper KillDisk is targeting financial organizations in Latin America.

▲ 1/16 Skygofree, a powerful Android spyware was discovered.

▲ 1/19 Skygofree targets LINE users in Japan.

▲ 1/18 Dridex banking Trojan compromises FTP sites.

▲ 1/29 ATM Jackpotting attacks hit the U.S for the first time.

▲ 3/15 The site that use the EC site construction framework Magento is exploited and malware LokiBot is spread via GitHub.

▲ 3/23 Malware SANNY is spread using malignant MS word macro.

▲ 3/27 GoScanSSH malware targets vulnerable SSH servers.

[N] Unauthorized handling of personal information on Facebook

▲ 3/17 Data analytics firm Cambridge Analytica illegally acquired private information from more than 50 million Facebook users and used it for the presidential election campaign.

▲ 3/20 British government authorities are investigating Cambridge Analytica.

▲ 3/21 Facebook CEO issued a statement.

▲ 3/26 The Federal Trade Commission (FTC) is investigating Facebook’s data practices.

▲ 3/27 The Japanese government will comply with the Personal Information Protection Act.

References (1/3)

(*1-1) 2018/3/27 サイバーセキュリティに関するグローバル動向四半期レポート（2017年10月～12月）を公開 ｜ NTTデータ
http://www.nttdata.com/jp/ja/news/information/2018/2018032701.html

(*1-2) 2018/3/8 ＮＥＭ不正流出、社員ＰＣのウイルス感染が原因と想定 ｜ 朝日新聞
https://www.asahi.com/articles/ASL386K55L38ULZU00D.html

(*1-3) 2017/11/5 NIC Asia Bank seeks CIB help to track down SWIFT server hacker | The Himalayan
https://thehimalayantimes.com/business/nic-asia-bank-seeks-cib-help-to-track-down-swift-server-hacker/

(*1-4) 2018/1/29 [コインチェック流出]その技術的ミスをNEM財団VPが語る 公式インタビュー全文翻訳 ｜ Business Insider Japan
https://www.businessinsider.jp/post-161098

(*1-5) 2018/2/3 Scammers Steal Over $1 Million Worth of Ethereum From Bee Token ICO Participants | Bleeping Computer https://www.bleepingcomputer.com/news/cryptocurrency/scammers-steal-over-1-million-worth-of-ethereum-from-bee-token-ico-participants/

(*1-6) 2018/1/23 新規仮想通貨公開による調達額、10%超が盗難に＝Ｅ＆Ｙ ｜ ロイター
https://jp.reuters.com/article/ico-ernst-young-idJPKBN1FC011

(*1-7) 2018/1/29 IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack | Bleeping Computer
https://www.bleepingcomputer.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishing-attack/

(*1-8) 2018/1/14 Hackers Hijack DNS Server of BlackWallet to Steal $400,000 | Bleeping Computer
https://www.bleepingcomputer.com/news/security/hackers-hijack-dns-server-of-blackwallet-to-steal-400-000/

(*1-9) 2018/2/27 Evrial: The Latest Malware That Steals Bitcoins Using the Clipboard | security affairs
http://securityaffairs.co/wordpress/69587/breaking-news/evrial-malware-steals-bitcoin.html

(*1-10) 2018/3/5 Sure, I’ll take that! New ComboJack Malware Alters Clipboards to Steal Cryptocurrency | Palo Alto Networks https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

(*1-11) 2018/1/3 NEW PYTHON-BASED CRYPTO-MINER BOTNET FLYING UNDER THE RADAR | F5 Networks
https://f5.com/labs/articles/threat-intelligence/malware/new-python-based-crypto-miner-botnet-flying-under-the-radar

(*1-12) 2018/1/31 What are “WannaMine” attacks, and how do I avoid them? | naked security by SOPHOS
https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/

(*1-13) 2018/2/1 DDG: A Mining Botnet Aiming at Database Servers | 360 Netlab Blog
https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-server-en/

(*1-14) 2018/2/4 Early Warning: ADB.Miner A Mining Botnet Utilizing Android ADB Is Now Rapidly Spreading | 360 Netlab Blog https://blog.netlab.360.com/early-warning-adb-miner-a-mining-botnet-utilizing-android-adb-is-now-rapidly-spreading-en/

(*1-15) 2018/1/31 Smominru Monero mining botnet making millions for operators | proofpoint
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

(*1-16) 2018/1/24 MyKings: 一个大规模多重僵尸网络 | 360 Netlab Blog https://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/

References (2/3)

(*1-17) 2018/3/22 インターネット観測結果等(平成29年) | 警察庁 http://www.npa.go.jp/cyberpolice/detect/pdf/20180322.pdf

(*1-18) 2017/4/24 NSAから流出のバックドア「DOUBLEPULSAR」、世界で感染急増 ｜ ZDNet Japan https://japan.zdnet.com/article/35100240/

(*1-19) 2017/6/28 ［特報］「WannaCry亜種に感染」、マクドナルド障害のマルウエア判明 ｜日経コンピュータ http://tech.nikkeibp.co.jp/it/atcl/news/17/062801786/

(*1-20) 2017/10/31 FIRSTHEALTH NETWORK DOWNTIME | FirstHealth of the Carolinas https://www.firsthealth.org/lifestyle/news-events/2017/10/network-downtime

(*1-21) 2018/1/22 当社社内システムにおけるランサムウェア感染と対処完了について｜NTTデータ http://www.nttdata.com/jp/ja/news/information/2018/2018012201.html

(*1-22) 2018/3/28 Boeing hit by WannaCry virus, but says attack caused little damage | The Seattle Times https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

(*1-23) Facts About the New Security Research Findings and Intel Products | intel https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

(*1-24) AMD Processor Security | AMD https://www.amd.com/en/corporate/security-updates

(*1-25) Arm Processor Security Update | arm https://developer.arm.com/support/security-update

(*1-26) 2018/3/29 Speculative Execution Exploit Performance Impacts - Describing the performance impacts to security patches for CVE-2017-5754 CVE-2017-5753 and CVE-2017-5715 | Red Hat https://access.redhat.com/articles/3307751

(*1-27) 2018/3/15 GitHub に 1 TBps 超の攻撃、「memcached」を利用する新たな DDoS 手法を解説 ｜ トレンドマイクロセキュリティブログ http://blog.trendmicro.co.jp/archives/17116

(*1-28) 2018/3/1 February 28th DDoS Incident Report | GitHub Engineering https://githubengineering.com/ddos-incident-report/

(*1-29) 2018/1/11 平昌オリンピックを標的とした不審な文書 ｜ マカフィー公式ブログ https://blogs.mcafee.jp/maliciousdocumenttargetspyeongchangolympics

(*1-30) 2018/2/16 平昌冬期五輪を、さらなるサイバー攻撃が襲った——マルウェア「Olympic Destroyer」の正体 ｜ WIRED https://wired.jp/2018/02/16/olympic-destroyer-malware/

(*1-31) 2018/1/16 Doctor Web detects infected games on Google Play with more than 4,500,000 downloads | Dr.WEB https://news.drweb.com/show/?i=11685&lng=en/

(*1-32) 2018/1/27 Hacker Compromised Official phpBB Download Links | Bleeping Computer https://www.bleepingcomputer.com/news/security/hacker-compromised-official-phpbb-download-links/

(*1-33) 2018/3/1 Doctor Web: over 40 models of Android devices delivered already infected from the manufacturers | Dr.WEB https://news.drweb.com/show/?i=11749&lng=en

References (3/3)

(*2-1) 2017/10/24 LokiBot Android Banking Trojan Turns Into Ransomware When You Try to Remove It | Bleeping Computer https://www.bleepingcomputer.com/news/security/lokibot-android-banking-trojan-turns-into-ransomware-when-you-try-to-remove-it/

(*2-2) 2018/1/24 Large Scale Monero Cryptocurrency Mining Operation using XMRig | Palo Alto Networks https://researchcenter.paloaltonetworks.com/2018/01/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig/

(*2-3) 2018/3/12 Mac Software Mines Cryptocurrency in Exchange for Free Access to Premium Account | The Hacker News https://thehackernews.com/2018/03/cryptocurrency-mining-software.html

(*2-4) 2018/3/12仮想通貨の採掘を秘密裏に行うツールをバンドルした「oCam」を窓の杜で収録中止　| 窓の杜 https://forest.watch.impress.co.jp/docs/news/1111067.html

(*2-5) 2018/3/7 Cryptocurrency miner now kills off other miners | SC Media UK https://www.scmagazineuk.com/cryptocurrency-miner-now-kills-off-other-miners/article/749242/

NTT DATA

Trusted Global Innovator