NTT DATA
Global IT Innovator

NTTDATA-CERT Global Security Trend Quarterly Report: October - December 2017

Mar 27th, 2018
NTT DATA Corporation

Table of Contents

NTT DATA

Executive Summary

In FY2017Q3 (October-December 2017), we witnessed an increase in attacks targeting cryptocurrency and a surge of IoT malware-infected devices in Japan.

The techniques of attack targeting cryptocurrency, such as drive-by mining, have become more diversified. In this report, we summarized the characteristics of diversified techniques of attack. This has been done based on comparative study of attacks targeting the traditional currencies so far.

The surge of IoT malware-infected devices in Japan may be incidental, however it cannot be denied that it may be also due to intentional attacks.

NTTDATA-CERT is concerned with the prevalence of malicious cryptocurrency mining* using the IoT botnet because both the attacks targeting cryptocurrency and the IoT malware-infected devices are increasing as mentioned above.

This report further provides a timeline of security-related events that occurred in FY2017Q3. We have reflected on the relevance of events by summarizing the events into topics.

* Cryptocurrency “Mining” is the process that uses machine resources such as PCs for adding transaction records to public ledger required for cryptocurrency transactions, and in return the miners are rewarded with cryptocurrency.

I. Hot Topic (1/4)

Increase in attacks targeting cryptocurrency (Timeline [A])

The attacks targeting cryptocurrency have become more diversified. Let us see the characteristics of the attacks targeting cryptocurrency.

■ The techniques of attacks targeting cryptocurrency are diversifying

The techniques of attacks targeting cryptocurrency have become more diversified. For example, in FY2017Q3, **"drive-by mining" which means mining cryptocurrency while browsing websites** has become a hot topic. In this report, we have summarized diversified techniques of attacks. Table 1 shows comparison of techniques of attacks targeting cryptocurrency and traditional currency.

■ Characteristics of attacks targeting cryptocurrency

The attacks targeting cryptocurrency can be classified into the attacks aiming at "PC user", "Service user", and "Service provider" respectively.

The peculiar attacks targeting cryptocurrency include **cryptocurrency mining done in an unauthorized manner using others' PC**((1) of Table 1) and **attacks during Initial Coin Offering (ICO)** ((2) of Table 1).

Recently, **Attackers' aim is shifting to cryptocurrency**. On one hand, unauthorized withdrawal and illegal money transfer using internet banking has decreased, on the other hand, illegal money transfer targeting cryptocurrency has increased (*1-1). And it was also reported that attacker groups have switched techniques of attack from ransomware to malicious cryptocurrency mining (*1-2).

Table 1 : Comparison of techniques of attacks targeting cryptocurrency and traditional currency

Aim	Cryptocurrency	Traditional currency
PC user	▪Cryptocurrency miner (1) ▪Drive-by mining	
Service user	Illegal money transfer by stealing authentication information (Banking malware, phishing etc.)	Illegal money transfer by stealing authentication information (Banking malware, phishing etc.)
	Attack on private key	Card counterfeiting
Service provider (Financial institution, cryptocurrency exchange etc.)	Unauthorized access to wallets of cryptocurrency exchanges	Illegal money transfer using SWIFT
	(Attack on cryptocurrency exchange machine)	Infect ATM with malware so as to withdraw the cash freely.
	Blackmail	Blackmail
	Attack during Initial Coin Offering (2)	

I. Hot Topic (2/4)

Spread of IoT malware infection (Timeline [B])

Why have IoT malware-infected devices surged in Japan?

■ Concerns about the increase in IoT malware-infected devices in Japan

In FY2017Q3, the surge of IoT malware-infected devices in Japan has become a hot topic (*1-3). When these infected devices are exploited to DDoS attacks originating from Japan, **total disconnection of communication from foreign IP addresses to take provisional measures against DDoS attacks will not be effective**. Since the increase in infected devices in Japan has become a serious threat, we examined the cause and the countermeasures. Figure 1 shows the scanning activity to 23/TCP and 52869/TCP observed by NICTER (*1-4).

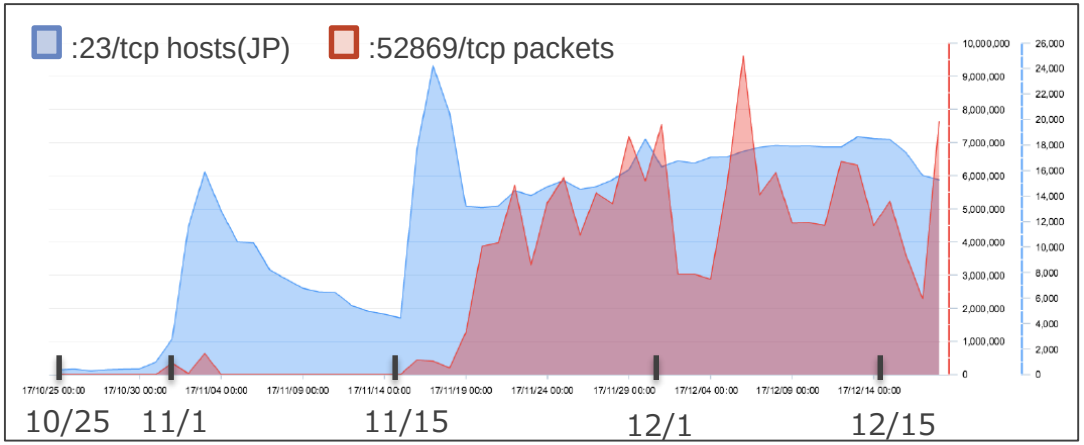


Figure 1 : Scanning activity to 23/TCP and 52869/TCP measured in Japan (infection spreading activity)

(Reference from "NICTER Analysis Report : Activities related to Mirai variant that spreads infection by exploiting the vulnerability in router" (*1-4))

■ Characteristics of IoT malware in this case

At the surge of IoT malware-infected devices, **the vulnerabilities in device were targeted** including backdoor account vulnerability in ZyXEL's modem (CVE-2016-10401) (*1-5), vulnerability in Realtek SDK (CVE-2014-8361), and vulnerability in Huawei's router (CVE-2017-17215) (*1-4).

■ Cause and countermeasures of surge in infected devices

The cause of surge might be that **the devices with vulnerability were incidentally rising in Japan**. But **there is also a possibility that an attacker intentionally targeted the devices in Japan** because in November, the scanning activity to 52869/TCP has been verified only in Japan (*1-6).

Currently, the IoT malware that spreads infection in Japan has targeted the existing vulnerabilities. Hence, in addition to the measures such as avoiding the usage of default ID/password, it is also needed to **apply patches**. Users of IoT devices such as routers and Web camera should check the patch on the manufacturer's website. Manufacturers should **consider incorporating security features such as avoid hardcoding ID/password in the design phase**. Ministry of Internal Affairs and Communications is considering to grant certification mark to IoT devices that fulfill certain security requirements. Newly manufactured IoT devices are expected to be secure against the attack of IoT malware (*1-7).

I. Hot Topic (3/4)
Other topics

■ Targeted attacks on financial institutions (Timeline [C])

(1) In FY2017Q3, there were unauthorized accesses to the banks and **illegal money transfer via SWIFT**.

- ✓ Early October : “Far Eastern International Bank” in Taiwan (*1-8)
- ✓ October 17th : “NIC Asia Bank” in Nepal (*1-9)

It was reported that the attack on the Far Eastern International Bank had features of the Lazarus Group (*1-10).

(2) In the attacks targeting financial institutions of former Soviet Union countries, attacker opened bank accounts using fictitious personal information. After a few months, the maximum amount of cashing was raised illegally through cyber attacks and cash was withdrawn from ATM (*1-11). **The technique is a combination of physical and cyber attacks**. Since legitimate ATM cards are used in this technique, it is difficult to detect this type of attack.

(3) **About 1 week after** the details about vulnerability in Equation Editor of Microsoft Office (CVE-2017-11882) were published and fixed (*1-12), the Cobalt group exploited that vulnerability to target the financial institutions in Russia and Turkey (*1-13).

■ Malware with capability to spread infection automatically

(1) A threat of malware that spreads infection like a worm is continuing. It was reported **that the number of detection of Qakbot and Emotet (information stealing Trojans), is increasing in the business users** (*1-14).

(2) A new infection-spreading ransomware, qkG, which seems in experimental phase, was also reported (*1-15). The qkG is not a fully automated self-expanding malware. It is needed that a user opens the encrypted file to spread the infection. When a user is infected, **a malicious macro is added to the Word standard template "normal.dot“**. When an infected user closes an unencrypted Word file, that file is encrypted. Besides encrypting the file, **a macro that runs automatically is added to the file** so as to spread the infection when other users open that file.

(3) It was reported that **IoT malware** Mirai variant had behaved like a worm after scanning activity (*1-16).

I. Hot Topic (4/4)
Other topics

■ Cyber blackmail (Timeline [F])

In October, the US Department of Education issued an alert against cyber blackmail (*1-17). At least 3 schools in the US have been threatened. The attacker stole students' personal information and **threatened that the personal information would be published or the attacker would harm the students if ransom request is not met**. There is a risk that the cyber blackmail against schools will increase in future even in Japan. The Ministry of Education, Culture, Sports, Science and Technology has published "Guidelines on Educational Information Security Policy" (*1-18).

■ Trend in email attacks (Timeline [H],[I],[J])

DDE (Dynamic Data Exchange) was exploited to spear phishing emails (*1-19) as well as malware spams (*1-20). DDE can spread malware regardless of whether macros are enabled or not. DDE is used to exchange data between applications and to issue commands on the Windows OS. The user can be tricked into clicking "Yes" on the popup while opening the file and thus trigger execution of the malicious code. Microsoft has published a security advisory against DDE (*1-21). Microsoft has provided a security patch to deactivate DDE in MS Word and Excel (*1-22).

Many instances were reported where **the user was tricked into clicking the malicious link in the body of email spoofing existing organization** (*1-23).

■ Business Email Compromise (Timeline [K])

Japan Airlines informed that it has been defrauded out of 384 Million yen (*1-24). It received an email supposing to be from an actual business partner stating that the bank account has been changed. The scammer had sent an invoice in PDF format closely resembling the official invoice. A closer look revealed the one-character difference between the sender's email address and the original email address (*1-25). The scammer was well versed with the contents of the invoice in the email thread. That makes it very clear that the scammer had secretly viewed the mails exchanged between the concerned persons.

The departments involved in money transfer should be aware of the fact that **they will encounter not only widely distributed attacks but also targeted attacks**. Also, it is necessary to ensure that the approval process for change in the transfer bank account is properly defined.

II. Forecast

Malicious cryptocurrency mining by IoT botnet becoming prevalent

■ Malicious cryptocurrency mining becoming prevalent

There are 2 major tricks to make others' PC mine cryptocurrency. One trick is **infect others' PC with "Cryptocurrency miner"**. It has been reported on the rise (*2-1). The other one is **"drive-by mining"** wherein a piece of JavaScript code is embedded into a Web page to perform cryptocurrency mining on the web browser of the user who visits the page. Coinhive service was launched in September and drive-by mining became prevalent using this service (*2-2). As mentioned in the topic, on one hand, illegal money transfer using internet banking has decreased, whereas on the other hand, illegal money transfer targeting cryptocurrency has increased (*1-1). Moreover, the attackers are switching from ransomware to cryptocurrency mining (*1-2). The target of mining cryptocurrency is not only servers or PCs but also the smartphones (*2-3).

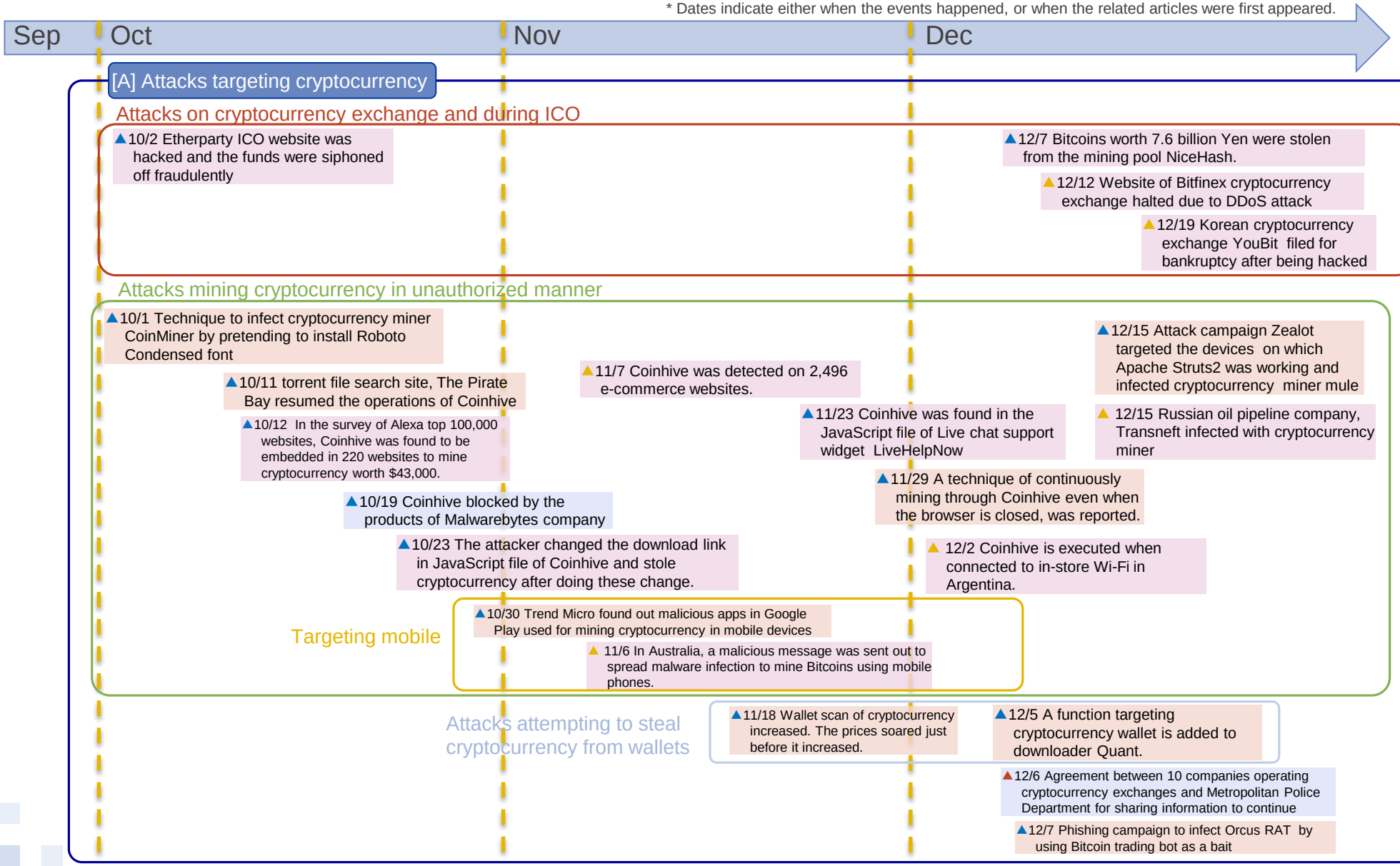
■ Cryptocurrency mining by IoT botnet becoming prevalent

NTTDATA-CERT anticipates that IoT botnet will be used for malicious cryptocurrency mining in future while IoT botnet is used mainly for DDoS attacks at present. Malicious cryptocurrency mining can reap a lot of benefits if it can be carried out for a "long time without being noticed" with "many" "high-performance devices". However, security measures such as antivirus software are often used in sophisticated devices such as servers and PCs thus making it difficult to mine for a long time without being noticed. Under such circumstances, it is assumed that **devices with some degree of sophistication are targeted for mining for a long time without being noticed**. IoT devices are considered to be less sophisticated, but there are also devices that require high performance like digital video recorder for video processing. The attackers might convert the IoT devices that fulfill the conditions of "being large in number", "with some degree of sophistication", and "connected to network for a long time and unlikely to be noticed" into bots and carry out malicious cryptocurrency mining. It was reported that around 6% of the communication regarding cryptocurrency mining was detected from household IoT devices (*2-4) and the evidences are already confirmed (*2-5). NTTDATA-CERT is concerned that this trend might become more prevalent in future.

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.



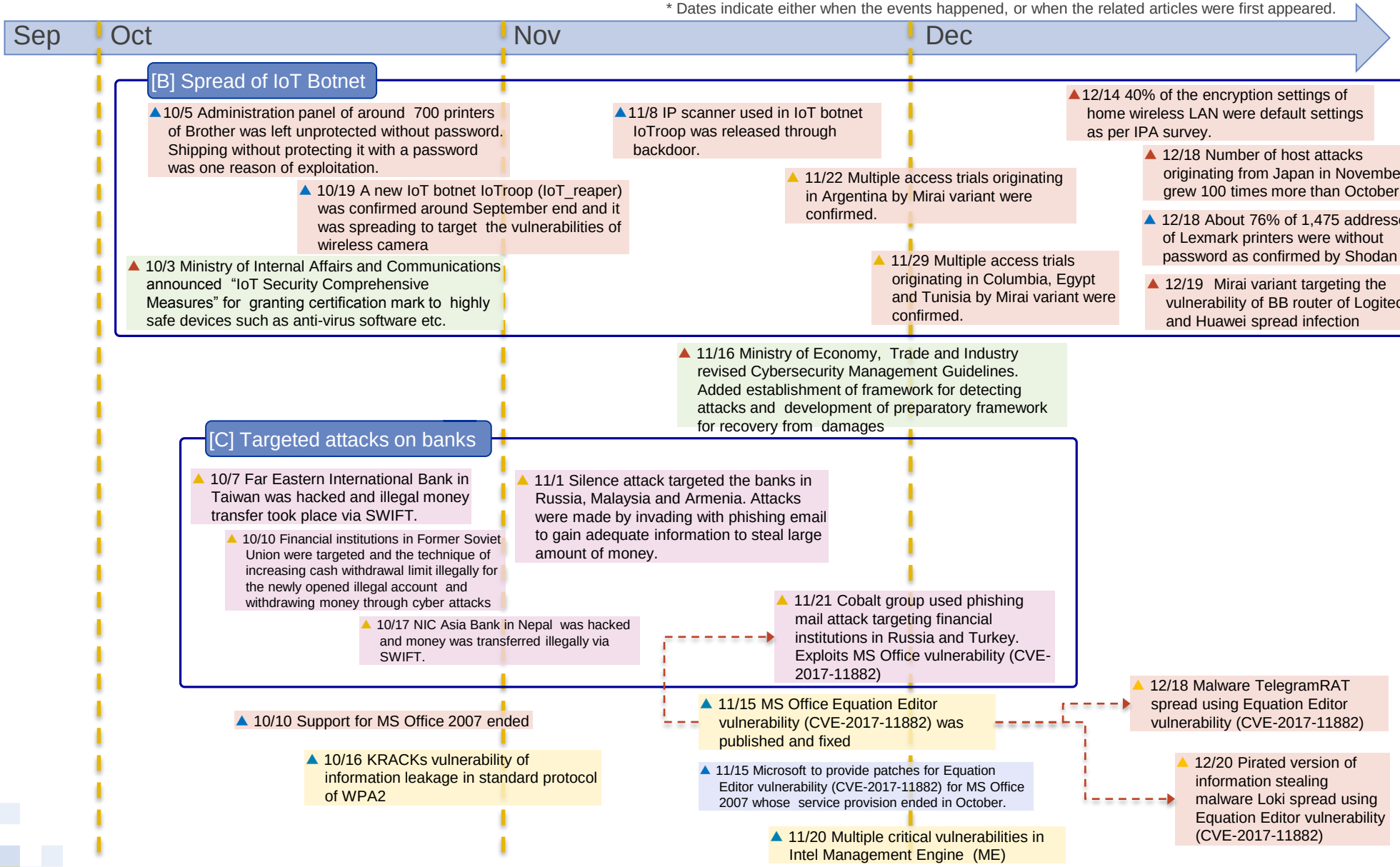
III. Timeline (2/9)

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

: Vulnerabilities
: Threats
: Cyber attacks/ Incidents

: Countermeasures
: Governments

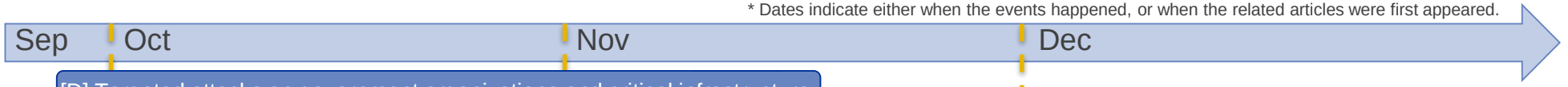
* Dates indicate either when the events happened, or when the related articles were first appeared.



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.



[D] Targeted attacks on government organizations and critical infrastructure

- ▲ 9/22 Spear phishing email attack targeted U.S. Electric Power companies
- ▲ 10/5 SYSCON Backdoor that uses FTP as C2 server, spread through phishing attack targeting the concerned persons of Red Cross and WHO
- ▲ 10/5 Attack campaign to spread FormBook malware for stealing information from defense, aeronautics, manufacturing contractors of US and Korea
- ▲ 10/6 A possible threat to hack White House Chief of Staff John Kelly's personal smartphone
- ▲ 10/10 Attacker group, OilRig attacked government agencies of UAE using Trojan ISMInjector
- ▲ 10/10 Data related to military capabilities such as details of fighter aircraft, military aircraft and naval vessels were stolen from Australian Intelligence Agency ASD
- ▲ 10/12 Attacker group, BRONZE BUTLER (alias Tick) stole confidential information such as Intellectual Property from Japanese organizations
- ▲ 10/10 Middle East attacker group BlackOasis exploited Adobe Flash vulnerability (CVE-2017-11292)
- ▲ 10/16 Adobe Flash vulnerability (CVE-2017-11292) was published and then fixed.
- ▲ 10/18 Attacks targeted government organizations, aerospace industry, etc. through APT 28 that exploited Adobe Flash (CVE - 2017 - 11292) vulnerability
- ▲ 10/22 APT28 created a phishing campaign to spread malware known as Seduploader using DDE in Word document designed specifically to target attendees of a security conference 'Cyber-Conflict' in US
- ▲ 10/20 US-CERT alerted of attacks targeting US government agencies and critical infrastructure
- ▲ 11/15 US-CERT published warning for Trojan Volgmer used by North Korean attacker group
- ▲ 12/21 US-CERT published warning for Trojan BANKSHOT used by North Korean attacker group

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.

Sep | Oct | Nov | Dec

[E] Ransomware attacks

Ransomware damage

- ▲ Early September Ransomware damage in Toshiba memory chips
- ▲ 10/3 Ransomware attack on the office of Englewood, Colorado
- ▲ 10/11 Ransomware attack on insurance companies that were forced to close down due to bankruptcy in August 2015. Their database was encrypted by Ransomware.
- ▲ 10/24 Ransomware BadRabbit caused damage in Russia, Ukraine etc.
- ▲ 10/25 Aika industry temporarily closed their website since it was used for spreading BadRabbit.
- ▲ 11/2 Phishing attack in Ukraine at the same time as the attack by Ransomware BadRabbit
- ▲ 11/16 Ransomware attack on Spring Hill City, Tennessee, US.
- ▲ 10/17 US medical institution group FirstHealth of the Carolinas infected with WannaCry variant. Company network was halted
- ▲ 12/8 Municipal PCs in Nashotah village, Wisconsin, US infected with Ransomware. They paid ransom for decrypting.

Variant

- ▲ 10/9 Attack to manually infect Ransomware BTCWare's new variant via RDP
- ▲ 10/13 Ransomware DoubleLocker that exploits Android accessibility service. It has a function to encrypt data and change PIN
- ▲ 10/16 Ransomware Tyrant spread in Iran
- ▲ 10/24 Android banking malware Lokibot turns into Ransomware and locks user's phone when the user tries to remove its admin privileges
- ▲ 10/29 Ransomware Sage 2.2 variant equipped with Sandbox avoidance and privilege upgrade function
- ▲ 11/7 Ransomware GIBON
- ▲ 11/9 Ransomware LockCrypt targeting servers. Spreads with RDP brute force attack.
- ▲ 11/22 Ransomware qkG that infects MS Word template to spread the infection. It was found to be in PoC stage in VirusTotal.
- ▲ 12/6 Attack to infect Ransomware HC7 via RDP. PsExec was used to spread infection across internal networks.
- ▲ 12/10 Ransomware Spider targeted mainly at areas like Bosnia, Herzegovina etc.
- ▲ 12/13 Ransomware CryptoMix variant ".WORK"

- ▲ 10/11 Sales of Ransomware increased by 2,502% on dark web between 2016 to 2017
- ▲ Mid-October Folder control access function released on Windows10
- ▲ 10/17 Decryption method of system encrypted with Petya variant (NotPetya). Manual operation was required based on the status of the target system
- ▲ 11/10 Monetary losses caused by Petya variant (NotPetya) exceeded $1 billion.
- ▲ 11/6 Number of detections of banking malware Qakbot and Emotet having worm function targeting enterprise users increased
- ▲ 12/11 26% of Ransomware targeting enterprise users increased to 23% as compared to last year.
- ▲ 12/20 Attacker group moved to mining of cryptocurrency using Ransomware VenusLocker

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.

Sep Oct Nov Dec

[F] Cyber blackmail

▲ 9/30 DDoS extortion group, Phantom Squad threatened companies all over the world with DDoS attacks

▲ 10/1 DB of Online Game Rainbow Six Siege statistical information provision service was stolen and ransom was demanded.

▲ 10/1 DDoS attack on English National Lottery.

▲ 11/4 Personal information of students was stolen and ransom was demanded from the network of University of Fraser Valley.

▲ 12/15 California voter information published on MongoDB was deleted and ransom was demanded.

The Dark Overlord attacked schools, medical institutions, and movie studios.

▲ 9/18 The attacker group, The Dark Overlord threatened the school district of Montana state in US

▲ 9/29 The attacker group, The Dark Overlord threatened the school district of Texas state in US

▲ 10/2 The attacker group, The Dark Overlord threatened the school district of Iowa state in US

▲ 10/16 The US Department of Education issued an alert against new threats carrying out cyber attacks.

▲ 10/18 The attacker group, The Dark Overlord illegally accessed American medical institution AMTA and stole patient information

▲ 10/24 The attacker group, The Dark Overlord intruded the network of plastic surgery clinic and stole confidential information and photographs

▲ 11/8 The attacker group, The Dark Overlord stole customer information from “Line204 “ Hollywood production studio

▲ 11/18 Partial data was deleted and ransom was demanded from Sacramento Department of Transportation, California.

[G] Attacks on critical infrastructure and industrial systems

▲ 10/11 DDoS attack on Swedish transportation system

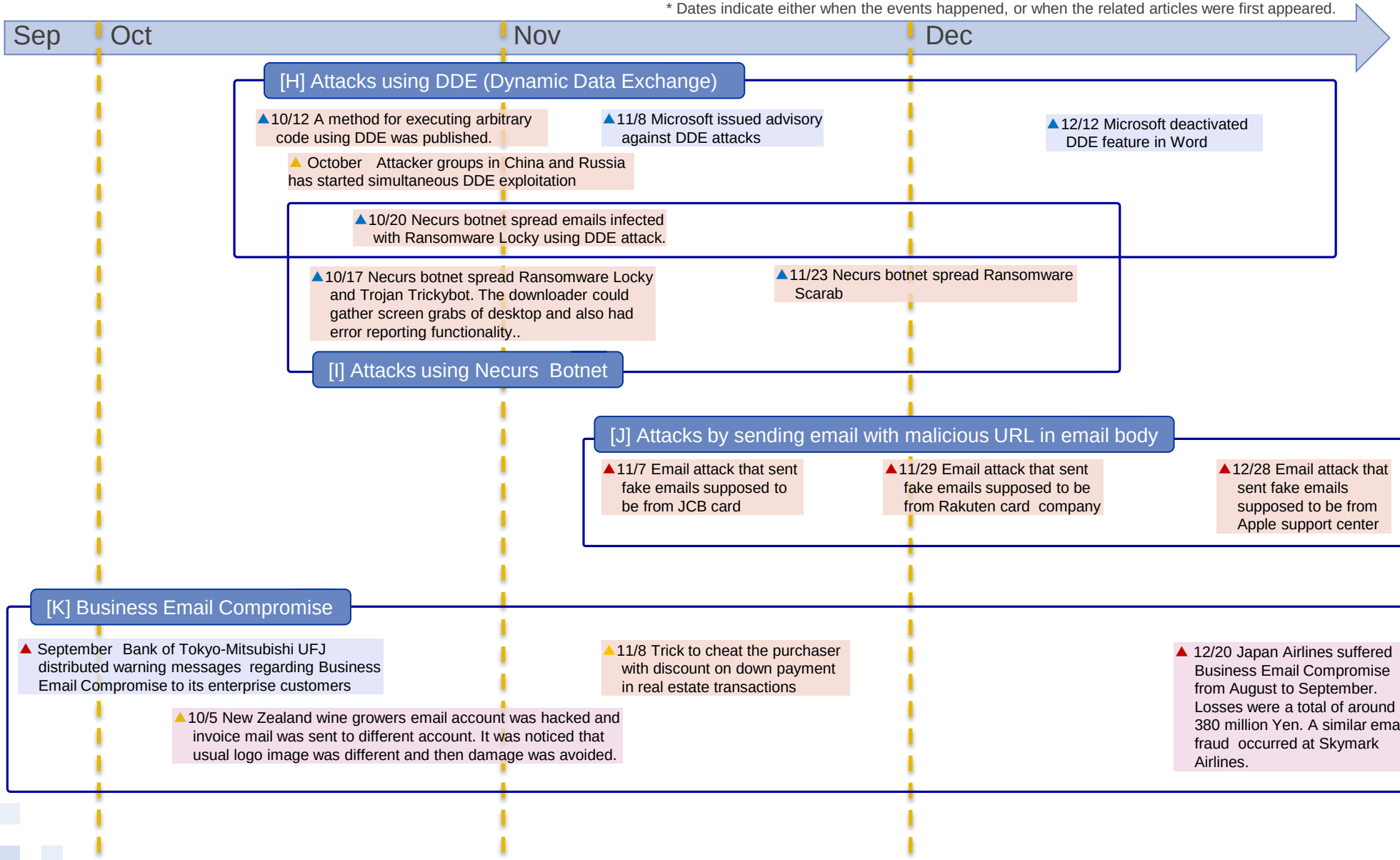
▲ 12/14 Malware Triton targeted Industrial control system

▲ 10/18 The Ministry of Education, Culture, Sports, Science and Technology published "Guidelines on Educational Information Security Policy"

III. Timeline (6/9)

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

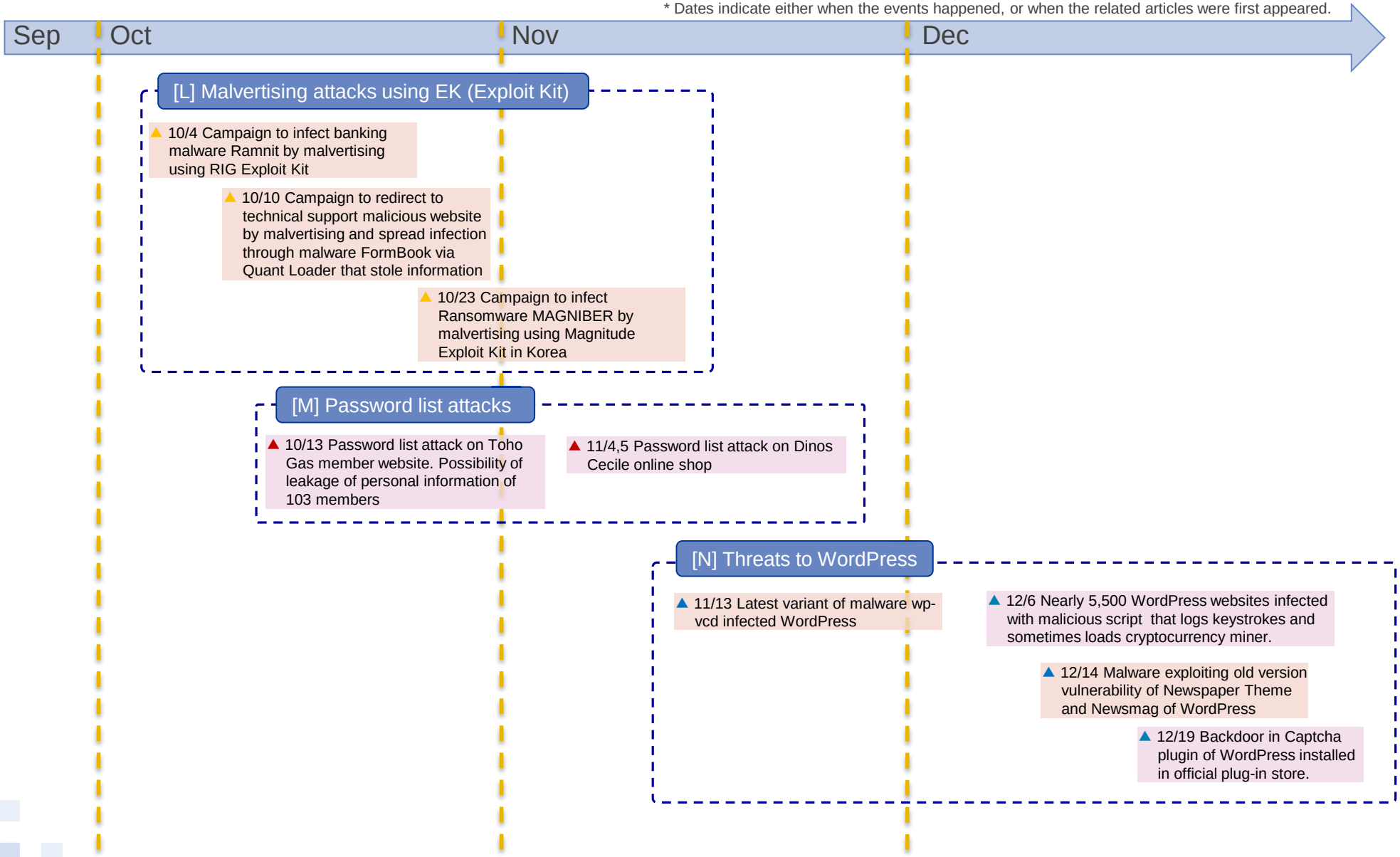
* Dates indicate either when the events happened, or when the related articles were first appeared.



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.



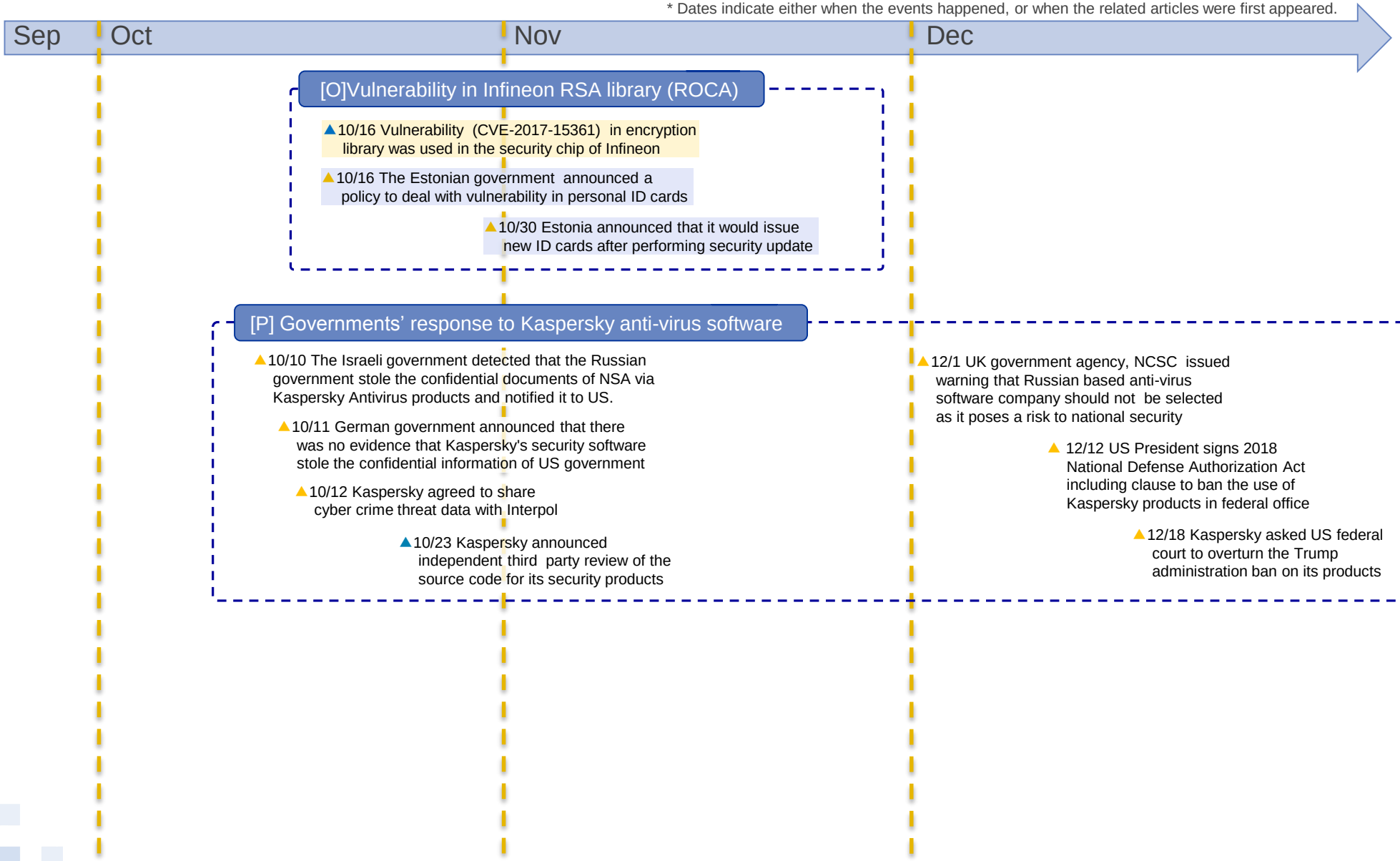
III. Timeline (8/9)

▲: 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.



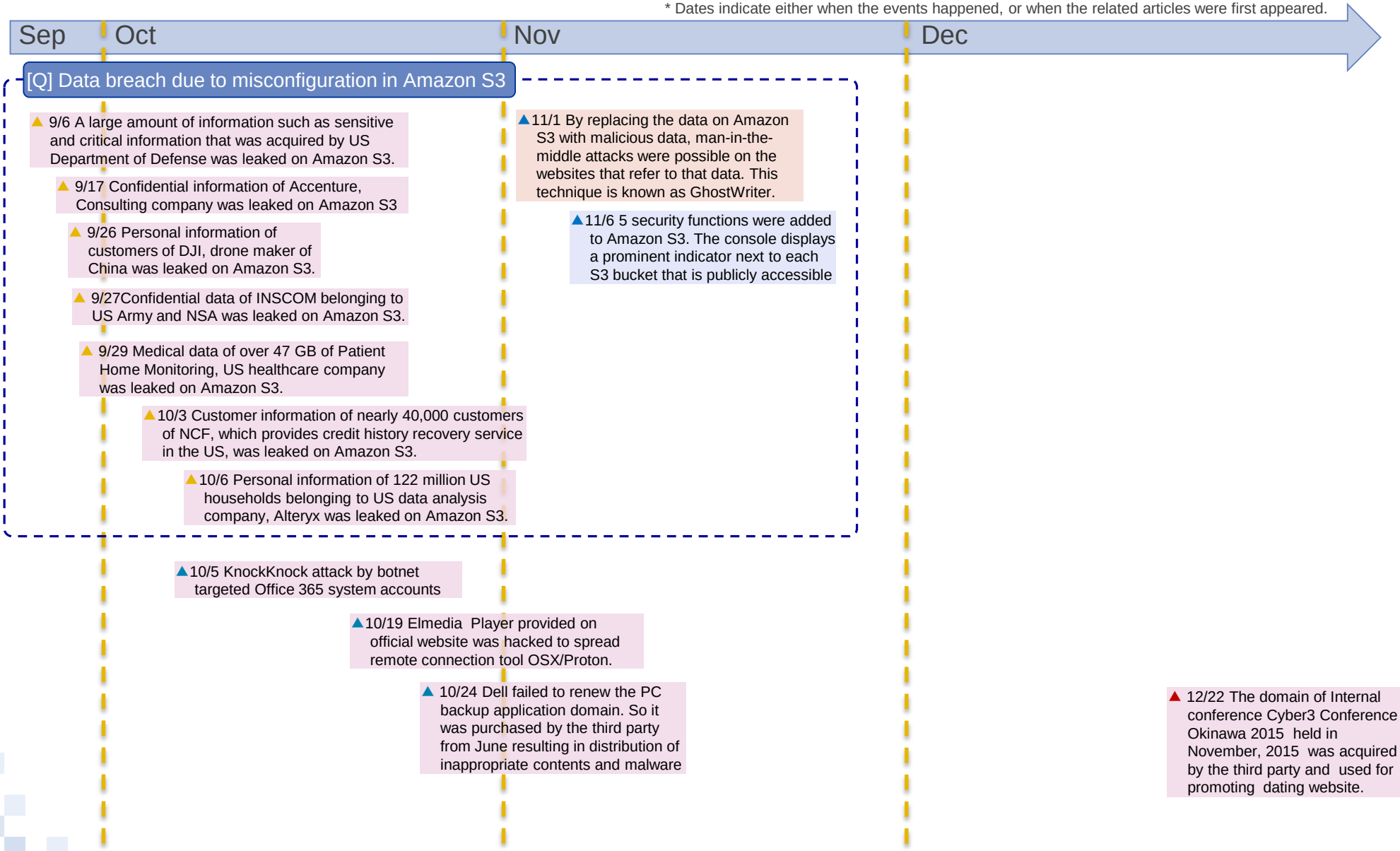
III. Timeline (9/9)

▲: 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.



References (1/2)

(*1-1) 2017/9/7 平成29年上半期におけるサイバー空間をめぐる脅威の情勢等について | 警察庁
http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf
(*1-2) 2017/12/20 Group Behind VenusLocker Switches From Ransomware to Monero Mining | FORTINET
https://blog.fortinet.com/2017/12/20/group-behind-venuslocker-switches-from-ransomware-to-monero-mining
(*1-3) 2017/12/19 Wi-Fi端末92万台感染も　ＩｏＴ狙うサイバー攻撃 |日本経済新聞
https://www.nikkei.com/article/DGXMZO24822170Z11C17A2TJ1000/
(*1-4) 2017/12/19 ルータ製品の脆弱性を悪用して感染を広げるMiraiの亜種に関する活動 | NICTER観測レポート http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf
(*1-5) 2017/12/7 国内における Mirai 亜種の感染急増 (2017年11月の観測状況) | IIJ-SECT https://sect.iij.ad.jp/d/2017/12/074702.html
(*1-6) 2018/1/18 インターネット定点観測レポート(2017年 10～12月) | JPCERT/CC https://www.jpcert.or.jp/tsubame/report/report201710-12.html
(*1-7) 2017/10/3「IoTセキュリティ総合対策」の公表 | 総務省 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html
(*1-8) 2017/10/7 Taiwanese bank tracing lost funds after hacker attacks | XINHUANET http://www.xinhuanet.com/english/2017-10/07/c_136663819.htm
(*1-9) 2017/11/5 NIC Asia Bank seeks CIB help to track down SWIFT server hacker | The Himalayan TIMES
https://thehimalayantimes.com/business/nic-asia-bank-seeks-cib-help-to-track-down-swift-server-hacker/
(*1-10) 2017/10/16 TAIWAN HEIST: LAZARUS TOOLS AND RANSOMWARE | BAE SYSTEMS THREAT RESEARCH BLOG
http://baesystemsai.blogspot.jp/2017/10/taiwan-heist-lazarus-tools.html
(*1-11) 2017/10/10 Post-Soviet Bank Heists: A Hybrid Cybercrime Study | SpiderLabs Blog
https://www.trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/
(*1-12) 2017/11/14 CVE-2017-11882 Microsoft Office Memory Corruption Vulnerability | Microsoft セキュリティ TechCenter
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2017-11882
(*1-13) 2017/11/28 Gaffe Reveals Full List of Targets in Spear Phishing Attack Using Cobalt Strike Against Financial Institutions | RISKIQ https://www.riskiq.com/blog/labs/cobalt-strike/
(*1-14) 2017/11/6 Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks | Microsoft Secure
https://cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/
(*1-15) 2017/11/27 Wordファイルの暗号化および自己複製機能を備えた暗号化型ランサムウェア「qkG」を確認 |トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/16463
(*1-16) 2017/12/5 Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869 | 360 netlab
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
(*1-17) 2017/10/16 ALERT! - CyberAdvisory - New Type of Cyber Extortion/Threat | Federal Student Aid
https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html

References (2/2)

(*1-18) 2017/10/18 教育情報セキュリティポリシーに関するガイドライン | 文部科学省
http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2017/10/18/1397369.pdf
(*1-19) 2017/11/7 Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack | McAfee
https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/
(*1-20) 2017/10/19 Necurs Botnet malspam pushes Locky using DDE attack | SANS ISC InfoSec Forums
https://isc.sans.edu/forums/diary/Necurs+Botnet+malspam+pushes+Locky+using+DDE+attack/22946/
(*1-21) 2017/12/13 マイクロソフト セキュリティ アドバイザリ 4053440 | Microsoft セキュリティ TechCenter
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx
(*1-22) 2017/12/12 ADV170021 Microsoft Office Defense in Depth Update | Microsoft Security TechCenter
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170021
(*1-23) 注意情報 2017年11月 | JC3 https://www.jc3.or.jp/topics/v_log/201711.html
(*1-24) 2017/12/20 日本航空、偽メールで３億８千万円詐欺被害 | 日本経済新聞
https://www.nikkei.com/article/DGXMZO24866680Q7A221C1CC1000/
(*1-25) 2017/12/22アドレス１字違い見逃す　日航3.8億円メール詐欺被害 | 日本経済新聞
https://www.nikkei.com/article/DGXMZO24979150S7A221C1EA5000/
(*2-1) 2017/9/12 Miners on the Rise | SECURELIST https://securelist.com/miners-on-the-rise/81706/
(*2-2) 2017/11/9 Exploit KitおよびScamサイトの衰退とCoinhiveの台頭 | wizSafe Security Signal
https://wizsafe.iij.ad.jp/2017/11/120/
(*2-3) 2017/10/30 Coin Miner Mobile Malware Returns, Hits Google Play | TrendLabs SECURITY INTELLIGENCE Blog
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/
(*2-4) 2017/11/30 2017年第3四半期セキュリティラウンドアップ サイバー犯罪者の狙いは仮想通貨に拡大 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/sr/sr-2017q3.html
(*2-5) 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

NTT DATA

Global IT Innovator