NTT DATA

Global IT Innovator

NTTDATA-CERT Global Security Quarterly Report:
July – September 2017

Nov 28th, 2017
NTT DATA Corporation

Table of Contents

Executive Summary

I. Overview (Global/Japan)

II. Hot Topic

Emergence of banking Trojan capable of spread infection automatically

III. Forecast

Emergence of banking Trojan aiming at reward points

IV. Timeline

Reference

Executive Summary

In FY2017Q2, we witnessed that banking Trojans gained additional functions and expanding target scope. These banking Trojans increase direct damage of stolen information as well as make incident response cumbersome and complicated; the cost of incident response grows considerable as well as damage and opportunity loss cannot be neglected. New banking Trojans also got to aim at cryptocurrency. NTTDATA-CERT anticipates that banking Trojans will go for reward points of loyalty programs as a new target.

This report provides timeline of security-related events that happened in FY2017Q2. Some events are aggregated on the basis of relevance, such as “Supply chain contamination” and “Data breach due to configuration error of Amazon S3.”

I. Overview (1/3)

Global

- **Ransomware and banking Trojan gained additional functions and expanded targets. (Timeline [A])**

  Two points to focus: one is additional functions and the other is expanding targets. Trojan Trickbot (*1-1) and Emotet (*1-2) have capability to spread infection automatically, for instance. We consider it happened due to WannaCry and NotPetya was broadly epidemic in the previous quarter. Banking Trojan also expanded targets: Dreambot started targeting cryptocurrency exchanges and wallets. (*1-3)

- **Contamination of software supply chain increased. (Timeline [B])**

  The contaminated version of CCleaner was distributed (*1-4). It contained malware despite legitimate signature appended. Software distributed by Korean company NetSarang Computer also contained malware (*1-5). Some Google Chrome Extensions were circulated containing malware due to the developer had been phished (*1-6).

- **Cryptocurrency miners on the rise. (Timeline [C])**

  According to Kaspersky, the number of users that have encountered miners has increased from 205,000 in 2013 to 1.65 million in 8 months of 2017. (*1-7) In another report, 61% of miner detection is in Asia. (*1-8) People who cannot afford millions of dollars were possibly victimized by abstraction of computing powers. (*1-9)

I. Overview (2/3)

- **Users’ carelessness and security misconfiguration caused data breach. (Timeline [F])**

  14 millions records of Verizon customers were published from Amazon S3 storage due to misconfigured security setting. (*1-10) Many dumped files of SQL database were confirmed to be accessible from the Internet by simply typing typical filenames. (*1-11) Some Google Groups were discovered exposing messages publicly that contain sensitive information. (*1-12)

- **145.5 millions of PII breached at Equifax.**

  Criminals exploited a known vulnerability of Apache Struts2, CVE-2017-5638, which was already fixed last March. (*1-13)

Japan

- **Password reuse attack aims at loyalty programs. (Timeline [I])**

  38 thousand-JPY-worth reward points Tokyo Gas loyalty program were stolen. (*1-14) One reason password reuse attack is effective is many users reuse ID and password. TrendMicro says 85.2% of Japanese users reuse passwords. (*1-15)

- **Compromise of EC software packages increased. (Timeline [J])**

  10 thousand credit card data were breached at 18 websites constructed with EC software Genesis-EC. Breach was first recognized last May. Data were stored inappropriately on the servers. (*1-16)

I. Overview (3/3)

- **Online extortion campaigns in rise. (Timeline [K])**

  Ransom DDoS (RDoS) continuously occurred since last quarter. On Sep 21, JPCERT/CC publicly alerted that multiple organizations received extortion emails by Phantom Squad, who requests money to stop DDoS. Multiple DDoS were observed in Japan since Sep 14, which JPCERT/CC did not confirm to be related to the extortions. Targets were banks and brokerages last June, Foreign Exchange operators and cryptocurrency exchanges in Sep, respectively. In these business the magnitude of loss in short-time service suspension is huge, thus they pay the ransom in higher probability.

- **Japan government enforces IoT security. (Timeline [L])**

  Ministry of Internal Affairs and Communications reportedly plans to introduce a security certification system for IoT devices which are manufactured domestically. (*1-18)(*1-19) MIAC is also supposed to assess vulnerabilities of IoT devices in current use. (*1-19)(*1-20) Likewise in the United States, a new bill was introduced that sets baseline security standards for the US government’s purchase of IoT devices. (*1-21)

  Since mid June, domestically-originated traffic to 22/tcp was increasingly observed; it is considered due to vulnerability exploit of Wi-Fi routers provided by NTT Docomo broadly. (*1-22)

II. Hot Topic (1/2)
Emergence of banking Trojan capable of spread infection automatically

How badly would you be affected in case your organization becomes infected with malware that is able to spread infection like a worm?

NTTDATA-CERT watch out for worm-like function of malware, which **requires no user's operations, regardless of the Internet connectivity, when expanding infection**. Once a single computer of your organization infected, it spreads among the intranet. Damage can be significant for corporates that have a number of computers in the intranet.

Recently this worm-like function is added to banking Trojans. Most Trojans of late such as DreamBot have key-logging function (*2-1) so **various data which are entered across the whole organization can be stolen including login credentials of multiple services**. You would have not only to reset banking service credentials but to reset all login credentials of other services. You would also need identify information possibly stolen from all infected computers. Financial cost, damage and opportunity loss through possible service suspension could be larger.

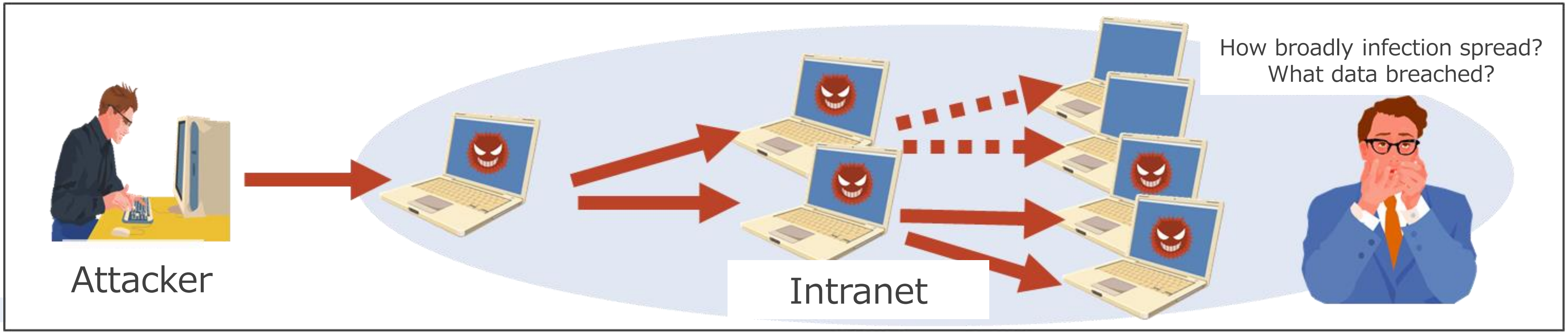


Image 1: Worm-like function of malware

II. Hot Topic (2/2)
Emergence of banking Trojan capable of spread infection automatically

How does malware spread infection?

There are two ways to spread infection: by exploiting vulnerabilities and by leveraging legitimate tools(*1) with stolen credentials. New trojans witnessed in this quarter use the latter. The former method is avoidable by simply applying patches and it is also highly detectable as time passes. Banking Trojans want to hide as persistently as possible until information is gained.

(*1) such as file share and remote management tools like PsExec and WMIC

To avoid infection, you should apply patches in a timely manner, disallow unnecessary file share, limit usage of remote management tools such as PsExec and WMIC, do appropriate authorization and access control, not reuse passwords, introduce behavior analysis, etc.

Chart 1: Methods applied to spread infection by each malware

Types of malware	Name of Malware	Methods to spread infection	
		Vulnerabilities	Legit tools with stolen credentials
Ransomware	WannaCry(*2-2)	✓	
	NotPetya (*2-3)	✓	✓
Banking Trojans	TrickBot*2(*1-1)		✓
	Emotet(*1-2)		✓

(*2) Trickbot is reported to try to add a worm-like function

III. Forecast
Emergence of banking Trojan aiming at reward points

■Banking Trojans targeting cryptocurrency. (Timeline [A])

Japan Cybercrime Control Center alerted last August that they are witnessing the shift of banking Trojans' target (*1-3)(*3-1): **Cybercriminals seemingly expand their target out of money.** In Japan the amount of money transferred maliciously is decreasing due to introduction of two-factor authentication (2FA) by users and anomaly detection by financial institutions. (*3-2) According to the fact that 87% of cryptocurrency wallets accessed maliciously did not leverage 2FA in the first half of 2017 (*3-2),cryptocurrency users are not used to 2FA. Additionally, cryptocurrency has been booming since 2016. (*3-1) No wonder cybercriminals are aiming at cryptocurrency now.

■Password reuse attacks continuously aim at reward points. (Timeline[I])

On the other hand, not a few press releases were seen last September in Japan such as Tokyo Gas, Bic Camera, and Rakuten. (*3-3) Password reuse by users cause the damage in such attacks: in order to login to Services A, attacker reuses ID/PW which were gained from Services B. Stolen points were actually exchanged to other kinds of points or e-cash and used to purchase items. Seeing this situation that those attacks have been reported since more than 4 years (*3-4) ago and never ceased, **users tend to have less sense of risk on reward points** than on money.

■What is the next target of banking Trojan?

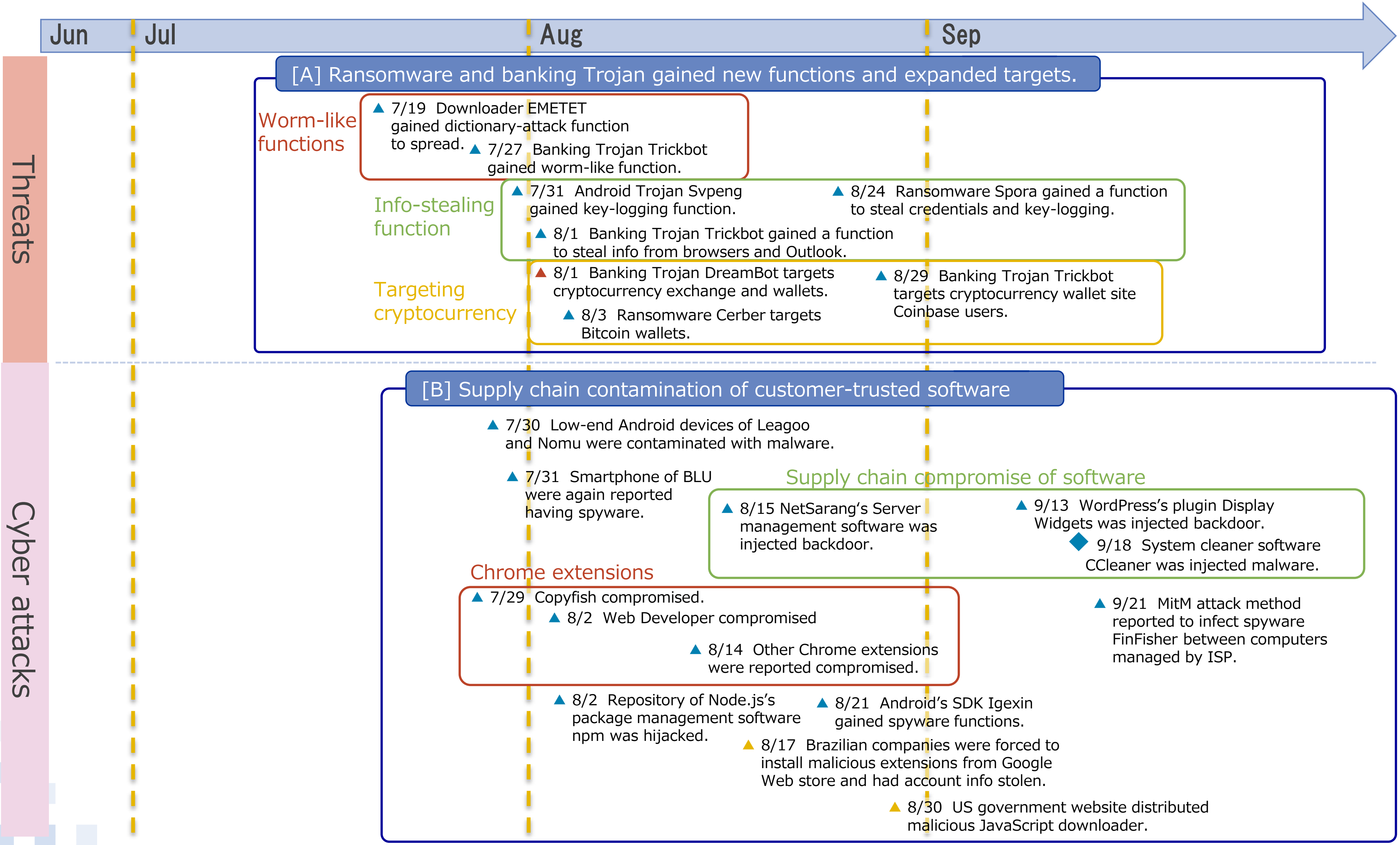
NTTDATA-CERT forecasts that we will see a **banking Trojan that aims at reward points** in the near future. If your computer is infected by such a malware and you login to any loyalty services, your credential is stolen and reward points are gone. Users should enable 2FA on loyalty service sites as a precaution. Services providers of loyalty service sites should prepare functions that enables users to check by themselves if there is any recent suspicious login.

IV. Timeline (1/6)

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

◆ : 10+ articles published
★ : 20+ articles published

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



[A] Ransomware and banking Trojan gained new functions and expanded targets.

Worm-like functions

▲ 7/19 Downloader EMETET gained dictionary-attack function to spread.

▲ 7/27 Banking Trojan Trickbot gained worm-like function.

Info-stealing function

▲ 7/31 Android Trojan Svpeng gained key-logging function.

▲ 8/1 Banking Trojan Trickbot gained a function to steal info from browsers and Outlook.

▲ 8/24 Ransomware Spora gained a function to steal credentials and key-logging.

Targeting cryptocurrency

▲ 8/1 Banking Trojan DreamBot targets cryptocurrency exchange and wallets.

▲ 8/3 Ransomware Cerber targets Bitcoin wallets.

▲ 8/29 Banking Trojan Trickbot targets cryptocurrency wallet site Coinbase users.

[B] Supply chain contamination of customer-trusted software

▲ 7/30 Low-end Android devices of Leagoo and Nomu were contaminated with malware.

▲ 7/31 Smartphone of BLU were again reported having spyware.

Supply chain compromise of software

▲ 8/15 NetSarang's Server management software was injected backdoor.

▲ 9/13 WordPress's plugin Display Widgets was injected backdoor.

◆ 9/18 System cleaner software CCleaner was injected malware.

Chrome extensions

▲ 7/29 Copyfish compromised.

▲ 8/2 Web Developer compromised

▲ 8/14 Other Chrome extensions were reported compromised.

▲ 9/21 MitM attack method reported to infect spyware FinFisher between computers managed by ISP.

▲ 8/2 Repository of Node.js's package management software npm was hijacked.

▲ 8/21 Android's SDK Igexin gained spyware functions.

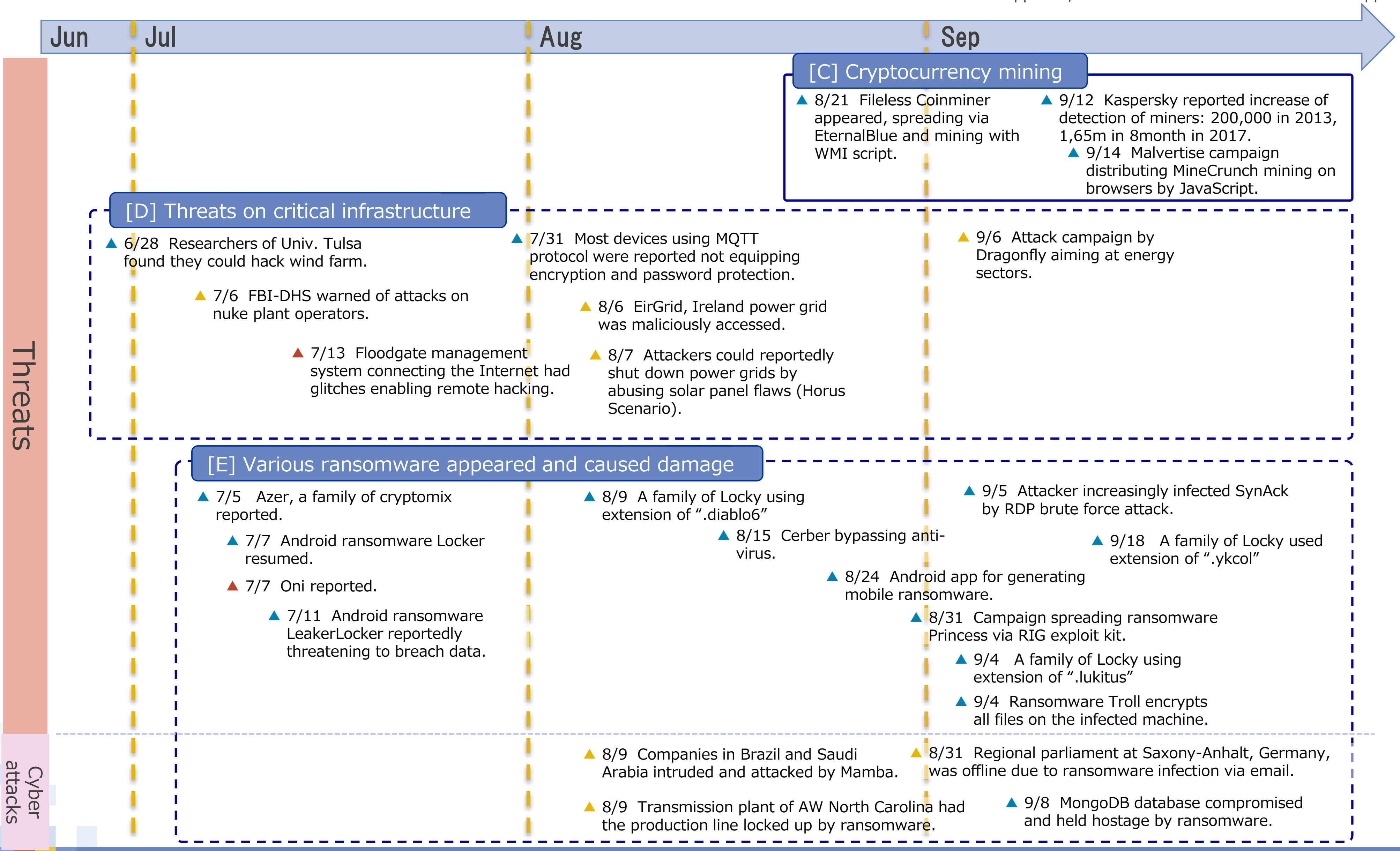
▲ 8/17 Brazilian companies were forced to install malicious extensions from Google Web store and had account info stolen.

▲ 8/30 US government website distributed malicious JavaScript downloader.

IV. Timeline (2/6)

▲ : Globally common
▲ : Specific regional
▲ : Domestic in Japan
◆ : 10+ articles published
★ : 20+ articles published

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



[C] Cryptocurrency mining

▲ 8/21 Fileless Coinminer appeared, spreading via EternalBlue and mining with WMI script.

▲ 9/12 Kaspersky reported increase of detection of miners: 200,000 in 2013, 1,65m in 8month in 2017.

▲ 9/14 Malvertise campaign distributing MineCrunch mining on browsers by JavaScript.

[D] Threats on critical infrastructure

▲ 6/28 Researchers of Univ. Tulsa found they could hack wind farm.

▲ 7/6 FBI-DHS warned of attacks on nuke plant operators.

▲ 7/13 Floodgate management system connecting the Internet had glitches enabling remote hacking.

▲ 7/31 Most devices using MQTT protocol were reported not equipping encryption and password protection.

▲ 8/6 EirGrid, Ireland power grid was maliciously accessed.

▲ 8/7 Attackers could reportedly shut down power grids by abusing solar panel flaws (Horus Scenario).

▲ 9/6 Attack campaign by Dragonfly aiming at energy sectors.

[E] Various ransomware appeared and caused damage

▲ 7/5 Azer, a family of cryptomix reported.

▲ 7/7 Android ransomware Locker resumed.

▲ 7/7 Oni reported.

▲ 7/11 Android ransomware LeakerLocker reportedly threatening to breach data.

▲ 8/9 A family of Locky using extension of ".diablo6"

▲ 8/15 Cerber bypassing anti-virus.

▲ 8/24 Android app for generating mobile ransomware.

▲ 8/31 Campaign spreading ransomware Princess via RIG exploit kit.

▲ 9/4 A family of Locky using extension of ".lukitus"

▲ 9/4 Ransomware Troll encrypts all files on the infected machine.

▲ 9/5 Attacker increasingly infected SynAck by RDP brute force attack.

▲ 9/18 A family of Locky used extension of ".ykcol"

▲ 8/9 Companies in Brazil and Saudi Arabia intruded and attacked by Mamba.

▲ 8/9 Transmission plant of AW North Carolina had the production line locked up by ransomware.

▲ 8/31 Regional parliament at Saxony-Anhalt, Germany, was offline due to ransomware infection via email.

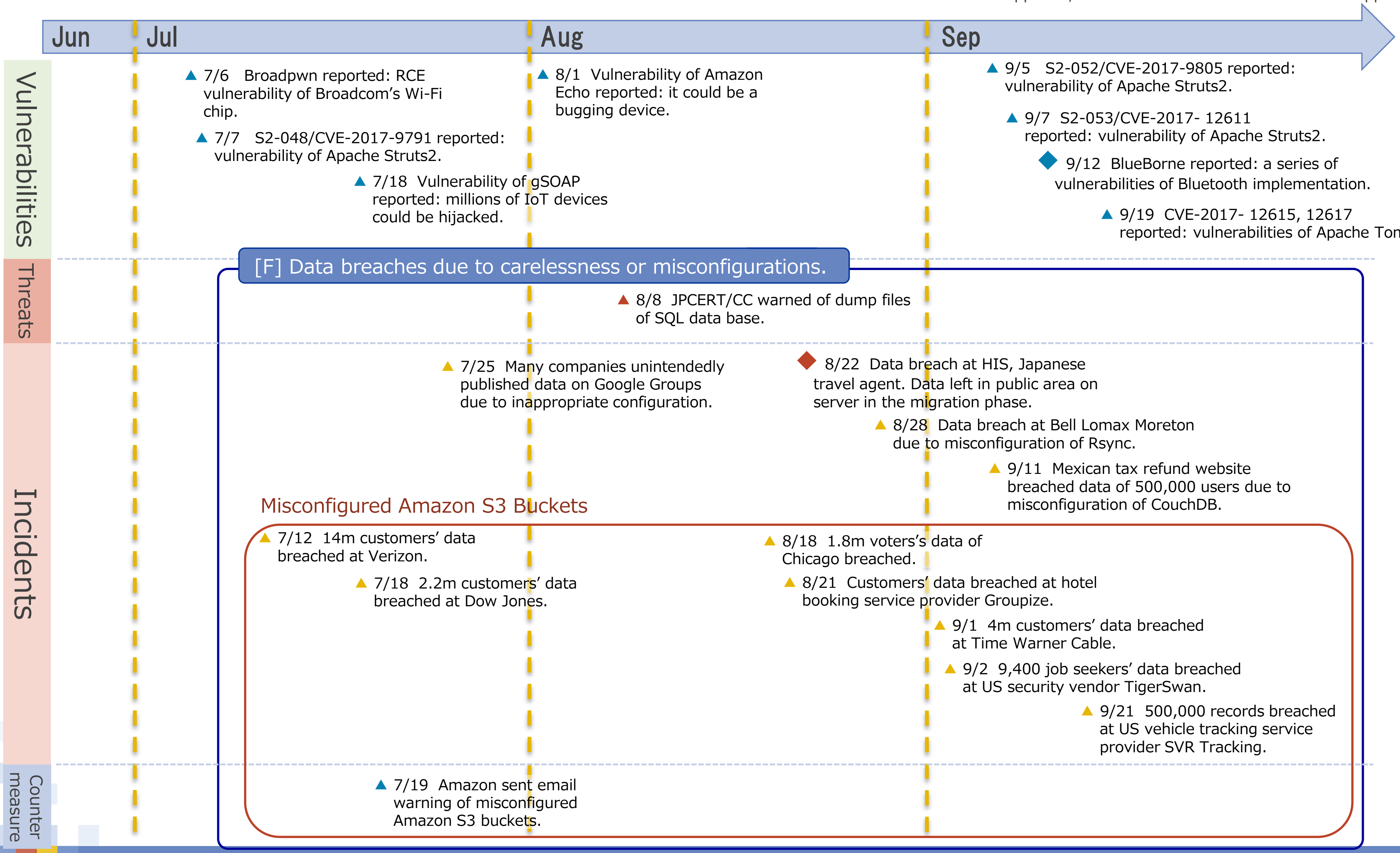
▲ 9/8 MongoDB database compromised and held hostage by ransomware.

IV. Timeline (3/6)

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

◆ : 10+ articles published
★ : 20+ articles published

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



Vulnerabilities

▲ 7/6 Broadpwn reported: RCE vulnerability of Broadcom's Wi-Fi chip.

▲ 7/7 S2-048/CVE-2017-9791 reported: vulnerability of Apache Struts2.

▲ 7/18 Vulnerability of gSOAP reported: millions of IoT devices could be hijacked.

▲ 8/1 Vulnerability of Amazon Echo reported: it could be a bugging device.

▲ 9/5 S2-052/CVE-2017-9805 reported: vulnerability of Apache Struts2.

▲ 9/7 S2-053/CVE-2017- 12611 reported: vulnerability of Apache Struts2.

◆ 9/12 BlueBorne reported: a series of vulnerabilities of Bluetooth implementation.

▲ 9/19 CVE-2017- 12615, 12617 reported: vulnerabilities of Apache Tomcat.

[F] Data breaches due to carelessness or misconfigurations.

Threats

▲ 8/8 JPCERT/CC warned of dump files of SQL data base.

Incidents

▲ 7/25 Many companies unintendedly published data on Google Groups due to inappropriate configuration.

◆ 8/22 Data breach at HIS, Japanese travel agent. Data left in public area on server in the migration phase.

▲ 8/28 Data breach at Bell Lomax Moreton due to misconfiguration of Rsync.

▲ 9/11 Mexican tax refund website breached data of 500,000 users due to misconfiguration of CouchDB.

Misconfigured Amazon S3 Buckets

▲ 7/12 14m customers' data breached at Verizon.

▲ 7/18 2.2m customers' data breached at Dow Jones.

▲ 8/18 1.8m voters's data of Chicago breached.

▲ 8/21 Customers' data breached at hotel booking service provider Groupize.

▲ 9/1 4m customers' data breached at Time Warner Cable.

▲ 9/2 9,400 job seekers' data breached at US security vendor TigerSwan.

▲ 9/21 500,000 records breached at US vehicle tracking service provider SVR Tracking.

Counter measure

▲ 7/19 Amazon sent email warning of misconfigured Amazon S3 buckets.

IV. Timeline (4/6)

▲ : Globally common
▲ : Specific regional
▲ : Domestic in Japan
◆ : 10+ articles published
★ : 20+ articles published

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

Jun | Jul | Aug | Sep

Threats

▲ 7/11 Adwind spread via spams: a RAT JavaScriprt-implemented and running on various OS.

▲ 8/1 ICS-CERT warned of Controller Area Network (CAN) bus vulnerability.

▲ 8/14 Disdain,new strain of exploit kit reported.

▲ 8/2 JS_POWMET, perfectly fileless malware reported.

[G] Attacks loading malicious contents from outside for bypass.

▲ 7/24 Users automatically download malicious Word template in opening attached file.

▲ 8/22 Ropemaker reported: forging received email via CSS located outside server.

▲ 9/18 Users automatically run PHP script hidden in a field of MS Word file when it opened.

Cyber attacks

▲ 7/4 Self-Service Food Kiosk Vendor Avanti hacked.

▲ 7/11 120m customers' data breached at Indian communication provider Reliance Jio.

▲ 8/11 APT28 using EternalBlue to attack hotels in Europe and Middle East.

▲ 8/16 Brute force attack against Scottish parliament.

▲ 8/22 Customers' data breached at Swedish hosting company Loopia.

▲ 8/30 2m customers' data breached at UK charity shop chain CeX.

▲ 9/4 28m users' data breached at Taringa!, SNS in South America.

▲ 9/6 230,000 credit card data stolen from ATMs in Korea.

★ 9/7 145.5m PPI breached at Equifax due to known vulnerability of Struts2.

[H] SMS phishing (Smishing)

▲ 8/14 Smishing campaign against US online banking users.

▲ 8/28 Smishing campaign against Korean users infecting Android banking Trojan MoqHao.

◆ 9/20 SEC discloses hackers penetrated internal system and profited in trading.

▲ 9/25 Email platform and clients' data of Deloitte hacked.

Incidents

▲ 7/24 Millions of PPI and confidential data of army breached at Swedish government system.

▲ 9/1 Secret email address and tel numbers breached at Instagram due to code errors.

Governments

▲ 7/11 Kaspersky omitted from federal supplier of US government.

▲ 7/12 Intelligence gathering bill passed parliament in Dutch.

▲ 8/18 US Cyber Command became a united combatant command.

▲ 9/13 US bans use of Kaspersky software in federal agencies.

▲ 9/7 EU defense ministers hold first exercises with NATO on cyber security.

countermeasures

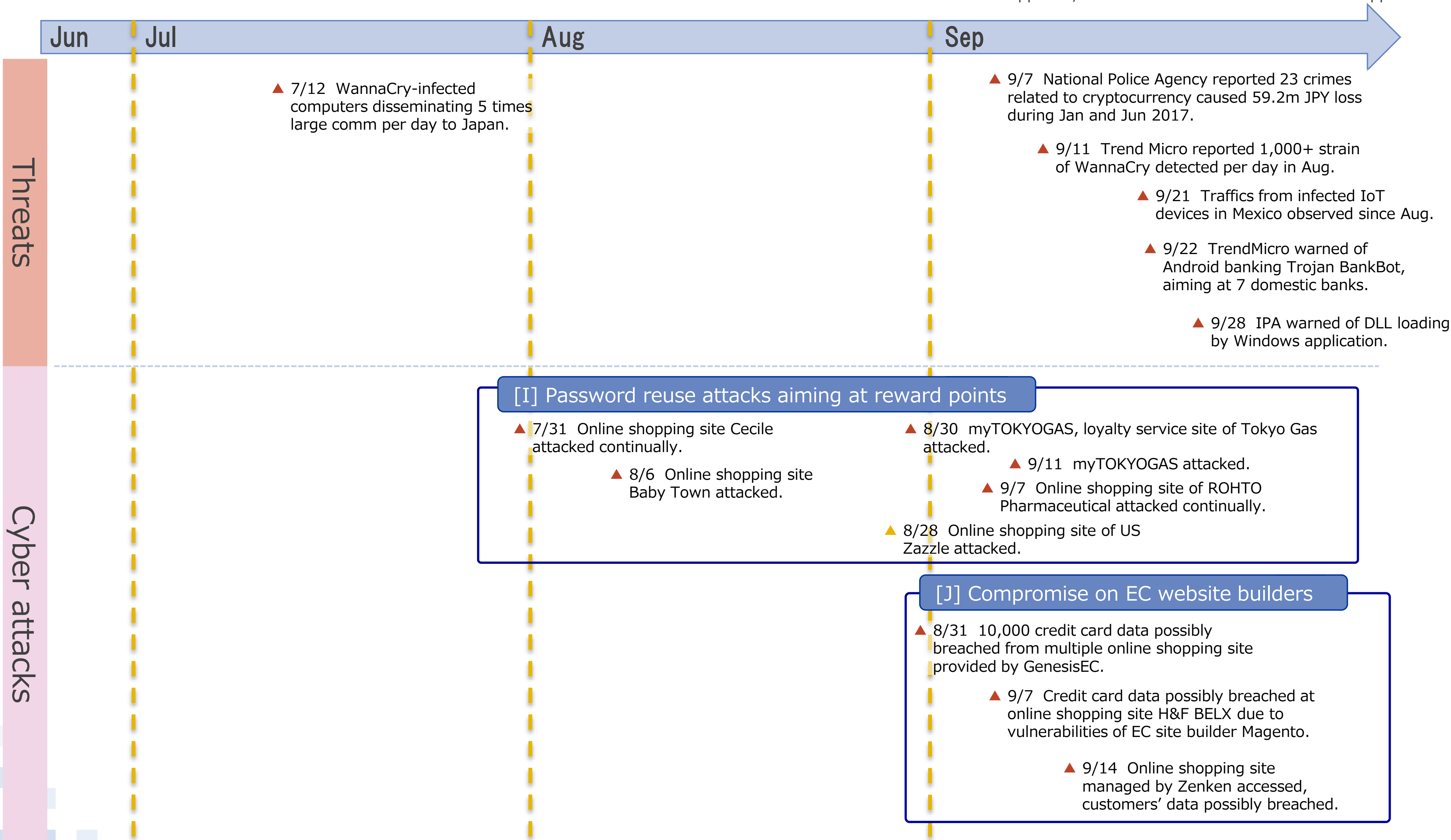
◆ 7/25 Adobe announced they will stop updating and distributing Flash Player at the end of 2020.

▲ 8/28 Tech companies cooperated to take down Android DDoS botnet WireX.

IV. Timeline (5/6)

▲ : Globally common
▲ : Specific regional
▲ : Domestic in Japan
◆ : 10+ articles published
★ : 20+ articles published

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



Threats

▲ 7/12 WannaCry-infected computers disseminating 5 times large comm per day to Japan.

▲ 9/7 National Police Agency reported 23 crimes related to cryptocurrency caused 59.2m JPY loss during Jan and Jun 2017.

▲ 9/11 Trend Micro reported 1,000+ strain of WannaCry detected per day in Aug.

▲ 9/21 Traffics from infected IoT devices in Mexico observed since Aug.

▲ 9/22 TrendMicro warned of Android banking Trojan BankBot, aiming at 7 domestic banks.

▲ 9/28 IPA warned of DLL loading by Windows application.

Cyber attacks

[I] Password reuse attacks aiming at reward points

▲ 7/31 Online shopping site Cecile attacked continually.

▲ 8/6 Online shopping site Baby Town attacked.

▲ 8/30 myTOKYOGAS, loyalty service site of Tokyo Gas attacked.

▲ 9/11 myTOKYOGAS attacked.

▲ 9/7 Online shopping site of ROHTO Pharmaceutical attacked continually.

▲ 8/28 Online shopping site of US Zazzle attacked.

[J] Compromise on EC website builders

▲ 8/31 10,000 credit card data possibly breached from multiple online shopping site provided by GenesisEC.

▲ 9/7 Credit card data possibly breached at online shopping site H&F BELX due to vulnerabilities of EC site builder Magento.

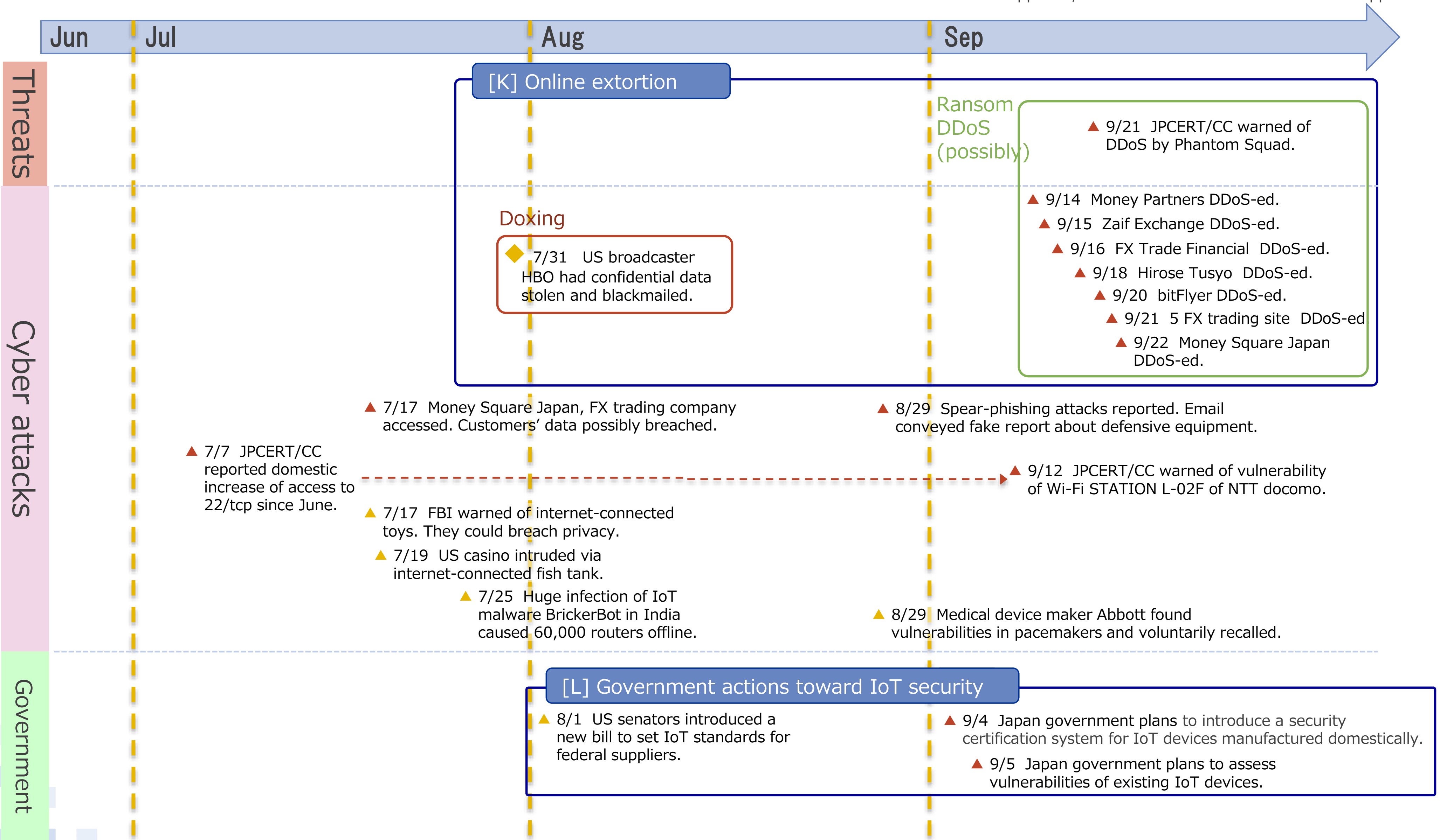
▲ 9/14 Online shopping site managed by Zenken accessed, customers' data possibly breached.

IV. Timeline (6/6)

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

◆ : 10+ articles published
★ : 20+ articles published

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



[K] Online extortion

Ransom DDoS (possibly)

▲ 9/21 JPCERT/CC warned of DDoS by Phantom Squad.

▲ 9/14 Money Partners DDoS-ed.

▲ 9/15 Zaif Exchange DDoS-ed.

▲ 9/16 FX Trade Financial DDoS-ed.

▲ 9/18 Hirose Tusyo DDoS-ed.

▲ 9/20 bitFlyer DDoS-ed.

▲ 9/21 5 FX trading site DDoS-ed

▲ 9/22 Money Square Japan DDoS-ed.

Doxing

◆ 7/31 US broadcaster HBO had confidential data stolen and blackmailed.

▲ 7/17 Money Square Japan, FX trading company accessed. Customers' data possibly breached.

▲ 8/29 Spear-phishing attacks reported. Email conveyed fake report about defensive equipment.

▲ 7/7 JPCERT/CC reported domestic increase of access to 22/tcp since June.

▲ 9/12 JPCERT/CC warned of vulnerability of Wi-Fi STATION L-02F of NTT docomo.

▲ 7/17 FBI warned of internet-connected toys. They could breach privacy.

▲ 7/19 US casino intruded via internet-connected fish tank.

▲ 7/25 Huge infection of IoT malware BrickerBot in India caused 60,000 routers offline.

▲ 8/29 Medical device maker Abbott found vulnerabilities in pacemakers and voluntarily recalled.

[L] Government actions toward IoT security

▲ 8/1 US senators introduced a new bill to set IoT standards for federal suppliers.

▲ 9/4 Japan government plans to introduce a security certification system for IoT devices manufactured domestically.

▲ 9/5 Japan government plans to assess vulnerabilities of existing IoT devices.

Reference (1/2)

(*1-1) 2017/7/27 New Version of “Trickbot” Adds Worm Propagation Module | FLASHPOINT blog
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/

(*1-2) 2017/7/19 Emotet takes wing with a spreader | threatgeek blog
https://www.fidelissecurity.com/threatgeek/2017/07/emotet-takes-wing-spreader

(*1-3) 2017/8/1　仮想通貨取引所等のウェブサイトがインターネットバンキングマルウェア「DreamBot」の標的となるおそれについて | 日本サイバー犯罪対策センター https://www.jc3.or.jp/topics/dces.html

(*1-4) 2017/9/18 Update to the CCleaner 5.33.6162 Security Incident | avast blog
https://blog.avast.com/update-to-the-ccleaner-5.33.6162-security-incident

(*1-5) 2017/8/7 Security Exploit in July 18, 2017 Build | NetSarang Computer
https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html

(*1-6) 2017/8/14 Threat actor goes on a Chrome extension hijacking spree | proofpoint
https://www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree

(*1-7) 2017/9/12 Miners on the Rise | SECURELIST https://securelist.com/miners-on-the-rise/81706/

(*1-8) Malwarebytes State of Malware Report 2017 | Malwarebytes
https://go.malwarebytes.com/StateofMalware0117.html

(*1-9) 2017/9/15 Despite the profitability of ransomware there is a good reason why mining malware is thriving | Virus Bulletin https://www.virusbulletin.com/blog/2017/09/despite-profitability-ransomware-there-good-reason-why-mining-malware-thriving/

(*1-10) 2017/7/12 Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts | UpGuard
https://www.upguard.com/breaches/verizon-cloud-leak

(*1-11) 2017/7/5 How 2,000 Unsecured Databases Landed on the Internet | ZEIT ONLINE
http://www.zeit.de/digital/datenschutz/2017-07/customer-data-how-2000-unsecured-databases-landed-online

(*1-12) 2017/7/24 Google Groups Misconfiguration Security Advisory | RedLock
https://blog.redlock.io/google-groups-misconfiguration

(*1-13) 2017/9/15 Equifaxの最大1億4300万人分の情報漏洩、原因は半年前のStruts2脆弱性 | ITpro
http://itpro.nikkeibp.co.jp/atcl/news/17/091502248/

(*1-14) 2017/9/22 ガス・電気料金情報ＷＥＢ照会サービス「myTOKYOGAS」への不正アクセスによるお客さま情報の流出ならびにポイントの不正使用について | 東京ガス http://www.tokyo-gas.co.jp/important/20170922-01.pdf

(*1-15) 2017/10/5 パスワードの利用実態調査 2017 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20171005-01.html

(*1-16) 2017/8/29 不正アクセスによるカード情報流出に関するお知らせとお詫び | ジェネシス・イーシー
http://www.genesis-ec.com/20170829.html

(*1-17) 2017/9/21 Phantom Squad を名乗る攻撃者からの DDoS 攻撃に関する情報 | JPCERT/CC
https://www.jpcert.or.jp/newsflash/2017092101.html

(*1-18) 2017/9/4　サイバー防衛で公的認証　総務省、ＩｏＴ総合対策 | 日本経済新聞
https://www.nikkei.com/article/DGXLASFS04H79_U7A900C1EE8000/

Reference (2/2)

(*1-19) 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

(*1-20) 2017/9/5 IoT機器に関する脆弱性調査等の実施 | 総務省
http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html

(*1-21) 2017/8/1 New Bill Seeks Basic IoT Security Standards | Krebs on Security
https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/

(*1-22) 2017/9/12 NTTドコモ Wi-Fi STATION L-02F の脆弱性に関する注意喚起 | JPCERT/CC
https://www.jpcert.or.jp/at/2017/at170034.html

(*2-1) マルウェア情報 DreamBot | 日本サイバー犯罪対策センター https://www.jc3.or.jp/info/malware.html

(*2-2) 2017/5/18 ランサムウェア「WannaCry／Wcry」のワーム活動を解析：侵入／拡散手法に迫る | トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/14920

(*2-3) 2017/6/30 話題のMBR破壊型ワームランサムウェアの内部構造を紐解く | MBSD Blog http://www.mbsd.jp/blog/20170630.html

(*3-1) 2017/8/4 新たに「ビットコイン」を狙う「URSNIF」を国内で確認 | トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/15633

(*3-2) 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

(*3-3) 2017/9/26 ポイント不正利用が相次ぐ 「リスト型攻撃」対策を | YOMIURI ONLINE
http://www.yomiuri.co.jp/science/goshinjyutsu/20170925-OYT8T50091.html

(*3-4) 2013/4/5 Tサイトへの不正ログインによるなりすまし被害のご報告およびパスワード変更のお願い | T-SITE
http://tsite.jp/cp/index.pl?xpg=PCIC0102&cp_id=6288

NTT DATA

Global IT Innovator