

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

Mar 27th, 2018 NTT DATA Corporation

Table of Contents

Executive Summary

- I. Hot Topic
- II. Forecast
- III. Timeline

References



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 loT botnet because both the attacks targeting cryptocurrency and the loT 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 <u>cryptocurrency mining done in an</u> <u>unauthorized manner using others' PC</u>((1) of Table 1) and <u>attacks during Initial Coin Offering</u> (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).

<u>Table 1 : Comparison of techniques of attacks targeting cryptocurrency and traditional currency</u>

Aim	Cryptocurrency	Traditional currency
PC user	-Cryptocurrency miner -Drive-by mining (1)	
Service user	Illegal money transfer by stealing authentication information (Banking malware, phishing etc.) Attack on private key	Illegal money transfer by stealing authentication information (Banking malware, phishing etc.) 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).

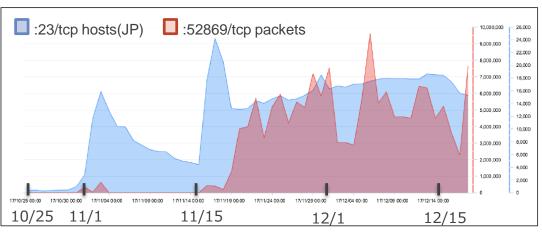


Figure 1 : Scanning activity to 23/TCP and 52869/TCP measured in Japan (infection spreading activity)

■ Characteristics of IoT malware in this case

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

At the surge of IoT malware-infected devices, <u>the vulnerabilities in device were targeted</u> 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) <u>About 1 week after</u> 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])

<u>DDE (Dynamic Data Exchange)</u> 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 <u>the user was tricked into clicking the malicious link in the body of email spoofing existing organization</u> (*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 <u>they will encounter not only widely</u> <u>distributed attacks but also targeted attacks</u>. 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 <u>infect others' PC with "Cryptocurrency miner"</u>. It has been reported on the rise (*2-1). The other one is <u>"drive-by mining"</u> 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
 : Vulnerabilities
 :: Countermeasures

 ▲: Specific regional
 :: Threats
 :: Governments

 ▲: Domestic in Japan
 :: Cyber attacks/

 Incidents

* Dates indicate either when the events happened, or when the related articles were first appeared. Sep Nov Oct Dec [A] Attacks targeting cryptocurrency Attacks on cryptocurrency exchange and during ICO ▲10/2 Etherparty ICO website was ▲12/7 Bitcoins worth 7.6 billion Yen were stolen hacked and the funds were siphoned from the mining pool NiceHash. off fraudulently ▲ 12/12 Website of Bitfinex cryptocurrency exchange halted due to DDoS attack ▲ 12/19 Korean cryptocurrency exchange YouBit filed for bankruptcy after being hacked Attacks mining cryptocurrency in unauthorized manner ▲ 10/1 Technique to infect cryptocurrency miner ▲ 12/15 Attack campaign Zealot CoinMiner by pretending to install Roboto targeted the devices on which Condensed font Apache Struts2 was working and △11/7 Coinhive was detected on 2.496 ▲10/11 torrent file search site. The Pirate infected cryptocurrency miner mule e-commerce websites. Bay resumed the operations of Coinhive 12/15 Russian oil pipeline company. ▲11/23 Coinhive was found in the ▲10/12 In the survey of Alexa top 100,000 JavaScript file of Live chat support Transneft infected with cryptocurrency websites, Coinhive was found to be widget LiveHelpNow miner embedded in 220 websites to mine cryptocurrency worth \$43,000. ▲11/29 A technique of continuously mining through Coinhive even when ▲10/19 Coinhive blocked by the the browser is closed, was reported. products of Malwarebytes company ▲10/23 The attacker changed the download link 12/2 Coinhive is executed when in JavaScript file of Coinhive and stole connected to in-store Wi-Fi in cryptocurrency after doing these change. Argentina. ▲ 10/30 Trend Micro found out malicious apps in Google Play used for mining cryptocurrency in mobile devices Targeting mobile ▲ 11/6 In Australia, a malicious message was sent out to spread malware infection to mine Bitcoins using mobile ▲ 12/5 A function targeting ▲11/18 Wallet scan of cryptocurrency Attacks attempting to steal increased. The prices soared just cryptocurrency wallet is added to cryptocurrency from wallets before it increased. downloader Quant. ▲12/6 Agreement between 10 companies operating cryptocurrency exchanges and Metropolitan Police Department for sharing information to continue ▲12/7 Phishing campaign to infect Orcus RAT by using Bitcoin trading bot as a bait

III. Timeline (2/9)

▲: Globally common

▲: Specific regional

▲: Domestic in Japan

: Vulnerabilities
: Threats
: Cyber attacks/

CountermeasuresGovernments

: Cyber attacks/ Incidents

* Dates indicate either when the events happened, or when the related articles were first appeared. Sep Nov Oct Dec [B] Spread of IoT Botnet ▲12/14 40% of the encryption settings of ▲ 10/5 Administration panel of around 700 printers ▲11/8 IP scanner used in IoT botnet home wireless LAN were default settings of Brother was left unprotected without password. IoTroop was released through as per IPA survey. Shipping without protecting it with a password backdoor. ▲ 12/18 Number of host attacks was one reason of exploitation. originating from Japan in November 11/22 Multiple access trials originating ▲ 10/19 A new IoT botnet IoTroop (IoT_reaper) grew 100 times more than October. in Argentina by Mirai variant were was confirmed around September end and it confirmed. ▲ 12/18 About 76% of 1.475 addresses was spreading to target the vulnerabilities of of Lexmark printers were without wireless camera password as confirmed by Shodan ▲ 11/29 Multiple access trials ▲ 10/3 Ministry of Internal Affairs and Communications originating in Columbia, Egypt announced "IoT Security Comprehensive ▲ 12/19 Mirai variant targeting the and Tunisia by Mirai variant were Measures" for granting certification mark to highly vulnerability of BB router of Logitech confirmed. safe devices such as anti-virus software etc. and Huawei spread infection ▲ 11/16 Ministry of Economy, Trade and Industry revised Cybersecurity Management Guidelines. Added establishment of framework for detecting attacks and development of preparatory framework for recovery from damages C] Targeted attacks on banks 10/7 Far Eastern International Bank in 11/1 Silence attack targeted the banks in Taiwan was hacked and illegal money Russia, Malaysia and Armenia, Attacks transfer took place via SWIFT. were made by invading with phishing email to gain adequate information to steal large 10/10 Financial institutions in Former Soviet amount of money. Union were targeted and the technique of increasing cash withdrawal limit illegally for the newly opened illegal account and 11/21 Cobalt group used phishing withdrawing money through cyber attacks mail attack targeting financial △ 10/17 NIC Asia Bank in Nepal was hacked institutions in Russia and Turkey. and money was transferred illegally via Exploits MS Office vulnerability (CVE-2017-11882) 12/18 Malware TelegramRAT ▲ 11/15 MS Office Equation Editor spread using Equation Editor ▲ 10/10 Support for MS Office 2007 ended vulnerability (CVE-2017-11882) was vulnerability (CVE-2017-11882) published and fixed ▲ 10/16 KRACKs vulnerability of 12/20 Pirated version of ▲ 11/15 Microsoft to provide patches for Equation information leakage in standard protocol information stealing Editor vulnerability (CVE-2017-11882) for MS Office of WPA2 malware Loki spread using 2007 whose service provision ended in October. Equation Editor vulnerability ▲ 11/20 Multiple critical vulnerabilities in (CVE-2017-11882) Intel Management Engine (ME)

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.

Sep Nov Oct Dec 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 ▲ 12/21 US-CERT published warning for Trojan BANKSHOT 10/20 US-CERT alerted of attacks 11/15 US-CERT published warning used by North Korean attacker targeting US government agencies for Trojan Volgmer used by North and critical infrastructure Korean attacker group group

III. Timeline (4/9)

▲: Globally common

▲: Specific regional

▲: Domestic in Japan

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

: Vulnerabilities : Threats

: Countermeasures : Governments

: Domestic in Japan : Cyber attacks/ Incidents

Sep Nov Oct Dec Ransomware attacks 10/24 Ransomware BadRabbit caused ▲ Early September Ransomware 12/8 Municipal PCs in Nashotah village, damage in Toshiba memory chips damage in Russia. Ukraine etc. Wisconsin, US infected with Ransomware. ▲ 10/3 Ransomware attack on the They paid ransom for decrypting. ▲ 10/25 Aika industry temporarily closed their office of Englewood, Colorado website since it was used for spreading BadRabbit 10/11 Ransomware attack on insurance ▲ 11/2 Phishing attack in Ukraine at the same companies that were forced to close down time as the attack by Ransomware BadRabbit due to bankruptcy in August 2015. Their ▲ 11/16 Ransomware attack on Spring Hill database was encrypted by Ransomware. City, Tennessee, US. ▲ 10/17 US medical institution group FirstHealth of the Carolinas infected with WannaCry Ransomware damage variant. Company network was halted ▲ 10/9 Attack to manually infect Ransomware ▲ 11/7 Ransomware GIBON ▲ 12/6 Attack to infect Ransomware HC7 BTCWare's new variant via RDP via RDP. PsExec was used to spread ▲ 11/9 Ransomware LockCrypt ▲ 10/13 Ransomware DoubleLocker infection across internal networks. targeting servers. Spreads with RDP that exploits Android accessibility ▲ 12/10 Ransomware Spider targeted brute force attack. service. It has a function to encrypt mainly at areas like Bosnia, data and change PIN ▲ 11/22 Ransomware qkG that Herzegovina etc. infects MS Word template to △ 10/16 Ransomware Tyrant spread in Iran ▲ 12/13 Ransomware spread the infection. It was found ▲ 10/24 Android banking malware CryptoMix variant ".WORK" to be in PoC stage in VirusTotal. 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 Variant and privilege upgrade function ▲ 10/11 Sales of Ransomware ▲ 12/11 26% of Ransomware targeting ▲ 11/10 Monetary losses caused by Petya increased by 2,502% on dark web variant (NotPetya) exceeded \$1 billion. enterprise users increased to 23% as between 2016 to 2017 compared to last year. ▲ Mid-October Folder control access ▲ 12/20 Attacker group moved to function released on Windows10 mining of cryptocurrency using Ransomware VenusLocker ▲ 10/17 Decryption method of system encrypted with Petya variant (NotPetya). Manual operation was required based on the status of the target system

▲ 11/6 Number of detections of banking malware Qakbot and Emotet having worm function targeting enterprise users increased

III. Timeline (5/9)

 ▲: Globally common
 : Vulnerabilities
 :: Countermeasures

 ▲: Specific regional
 :: Threats
 :: Governments

 ▲: Domestic in Japan
 :: Cyber attacks/

 Incidents
 Incidents

* 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 11/4 Personal information of 12/15 California voter information students was stolen and ransom was published on MongoDB was deleted Squad threatened companies all over the world with DDoS attacks demanded from the network of and ransom was demanded. University of Fraser Valley. ▲ 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. The Dark Overlord attacked schools, medical institutions, and movie studios. 9/18 The attacker group, The ▲ 10/16 The US Department of Education Dark Overlord threatened the issued an alert against new threats school district of Montana state carrying out cyber attacks. in US 10/18 The attacker group, The Dark 11/8 The attacker group, The Dark Overlord illegally accessed American Overlord stole customer information from 9/29 The attacker group, The Dark medical institution AMTA and stole "Line204 " Hollywood production studio Overlord threatened the school district of Texas state in US patient information 10/2 The attacker group, The 10/24 The attacker group, The Dark Overlord Dark Overlord threatened the intruded the network of plastic surgery clinic and school district of Iowa state in US stole confidential information and photographs 11/18 Partial data was deleted and ransom was demanded from Sacramento Department of Transportation, California. 10/11 DDoS attack on Swedish ▲ 12/14 Malware Triton targeted Industrial control system transportation system [G] Attacks on critical infrastructure and industrial systems ▲ 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
□: Countermeasures
□: Governments
□: Cyber attacks/

Incidents

* Dates indicate either when the events happened, or when the related articles were first appeared. Sep Oct Nov Dec [H] Attacks using DDE (Dynamic Data Exchange) ▲10/12 A method for executing arbitrary ▲11/8 Microsoft issued advisory ▲ 12/12 Microsoft deactivated code using DDE was published. against DDE attacks DDE feature in Word △ October Attacker groups in China and Russia has started simultaneous DDE exploitation ▲10/20 Necurs botnet spread emails infected with Ransomware Locky using DDE attack. ▲11/23 Necurs botnet spread Ransomware ▲10/17 Necurs botnet spread Ransomware Locky Scarab and Trojan Trickybot. The downloader could gather screen grabs of desktop and also had error reporting functionality... [I] Attacks using Necurs Botnet [J] Attacks by sending email with malicious URL in email body ▲11/7 Email attack that sent ▲11/29 Email attack that sent ▲12/28 Email attack that fake emails supposed to fake emails supposed to be sent fake emails be from JCB card from Rakuten card company supposed to be from Apple support center [K] Business Email Compromise ▲ September Bank of Tokyo-Mitsubishi UFJ 11/8 Trick to cheat the purchaser ▲ 12/20 Japan Airlines suffered distributed warning messages regarding Business with discount on down payment **Business Email Compromise** Email Compromise to its enterprise customers in real estate transactions from August to September. Losses were a total of around △10/5 New Zealand wine growers email account was hacked and 380 million Yen. A similar email invoice mail was sent to different account. It was noticed that fraud occurred at Skymark usual logo image was different and then damage was avoided. Airlines.

III. Timeline (7/9)

 ▲: Globally common
 : Vulnerabilities
 :: Countermeasures

 ▲: Specific regional
 :: Threats
 :: Governments

 ▲: Domestic in Japan
 :: Cyber attacks/

Incidents

* Dates indicate either when the events happened, or when the related articles were first appeared. Sep Oct Nov Dec [L] Malvertising attacks using EK (Exploit Kit) 10/4 Campaign to infect banking malware Ramnit by malvertising using RIG Exploit Kit 10/10 Campaign to redirect to technical support malicious website by malvertising and spread infection through malware FormBook via Quant Loader that stole information 10/23 Campaign to infect Ransomware MAGNIBER by malvertising using Magnitude Exploit Kit in Korea [M] Password list attacks ▲ 11/4,5 Password list attack on Dinos ▲ 10/13 Password list attack on Toho Gas member website. Possibility of Cecile online shop leakage of personal information of 103 members

[N] Threats to WordPress

- ▲ 11/13 Latest variant of malware wpvcd infected WordPress
- ▲ 12/6 Nearly 5,500 WordPress websites infected with malicious script that logs keystrokes and sometimes loads cryptocurrency miner.
 - ▲ 12/14 Malware exploiting old version vulnerability of Newspaper Theme and Newsmag of WordPress
 - ▲ 12/19 Backdoor in Captcha plugin of WordPress installed in official plug-in store.

III. Timeline (8/9)

▲: Globally common

▲: Specific regional

▲: Domestic in Japan

: Vulnerabilities
: Threats
: Cyber attacks/

: Countermeasures : Governments

Incidents

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

Sep Oct Nov Dec [O]Vulnerability in Infineon RSA library (ROCA) ▲10/16 Vulnerability (CVE-2017-15361) in encryption library was used in the security chip of Infineon △10/16 The Estonian government announced a policy to deal with vulnerability in personal ID cards ▲ 10/30 Estonia announced that it would issue new ID cards after performing security update [P] Governments' response to Kaspersky anti-virus software △10/10 The Israeli government detected that the Russian 12/1 UK government agency, NCSC issued government stole the confidential documents of NSA via warning that Russian based anti-virus Kaspersky Antivirus products and notified it to US. software company should not be selected as it poses a risk to national security △10/11 German government announced that there was no evidence that Kaspersky's security software △ 12/12 US President signs 2018 stole the confidential information of US government National Defense Authorization Act including clause to ban the use of △10/12 Kaspersky agreed to share Kaspersky products in federal office cyber crime threat data with Interpol ▲ 12/18 Kaspersky asked US federal ▲10/23 Kaspersky announced court to overturn the Trump independent third party review of the administration ban on its products source code for its security products

III. Timeline (9/9)

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

: Threats : Cyber attacks/

: Vulnerabilities : Countermeasures : Governments

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

Sep Nov Dec Oct [Q] Data breach due to misconfiguration in Amazon S3 ▲11/1 By replacing the data on Amazon 9/6 A large amount of information such as sensitive S3 with malicious data, man-in-theand critical information that was acquired by US middle attacks were possible on the Department of Defense was leaked on Amazon S3. websites that refer to that data. This 9/17 Confidential information of Accenture. technique is known as GhostWriter. Consulting company was leaked on Amazon S3 ▲11/6 5 security functions were added 9/26 Personal information of to Amazon S3. The console displays customers of DJI, drone maker of a prominent indicator next to each China was leaked on Amazon S3. S3 bucket that is publicly accessible 9/27Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3. 9/29 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3. ▲ 10/3 Customer information of nearly 40,000 customers of NCF, which provides credit history recovery service in the US, was leaked on Amazon S3. ▲ 10/6 Personal information of 122 million US households belonging to US data analysis company. Alteryx was leaked on Amazon S3. ▲10/5 KnockKnock attack by botnet targeted Office 365 system accounts ▲10/19 Elmedia Player provided on official website was hacked to spread remote connection tool OSX/Proton. ▲ 10/24 Dell failed to renew the PC ▲ 12/22 The domain of Internal backup application domain. So it conference Cyber3 Conference was purchased by the third party Okinawa 2015 held in from June resulting in distribution of November, 2015 was acquired inappropriate contents and malware by the third party and used for promoting dating website.

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 I o T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 news/01ryutsu03_02000126.html

http://www.soumu.go.jp/menu_news/s-

- (*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-2017g3.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

NTTData

Global IT Innovator