# 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 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, Attacker's 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

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

---

*(1)* - 1: *Attacker's aim is shifting to cryptocurrency*

*(2)* - 2: *Attacker groups have switched techniques of attack from ransomware to malicious cryptocurrency mining*
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).

- 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)

**A: Attacks targeting cryptocurrency**

### Attacks on cryptocurrency exchange and during ICO
- 10/2 Etherparty ICO website was hacked and the funds were siphoned off fraudulently.
- 10/11 Torrent file search site, The Pirate Bay resumed the operations of Coinhive.
- 10/12 In the survey of Alexa top 100,000 websites, Coinhive was found to be embedded in 220 websites to mine cryptocurrency worth $43,000.
- 10/1 Coinhive was detected on 2,496 e-commerce websites.
- 10/19 Coinhive blocked by the products of Malwarebytes company.
- 10/23 The attacker changed the download link in JavaScript file of Coinhive and stole cryptocurrency after doing these change.
- 12/7 Bitcoins worth 7.6 billion Yen were stolen from the mining pool NiceHash.
- 12/23 Coinhive was found in the JavaScript file of Live chat support widget LiveHelpNow.
- 12/29 A technique of continuously mining through Coinhive even when the browser is closed, was reported.
- 12/2 Coinhive is executed when connected to in-store Wi-Fi in Argentina.
- 12/15 Russian oil pipeline company, Transneft infected with cryptocurrency miner.
- 12/15 Attack campaign Zealot targeted the devices on which Apache Struts2 was working and infected cryptocurrency miner mule.
- 12/12 Website of Bitfinex cryptocurrency exchange halted due to DDoS attack.
- 12/1 Korean cryptocurrency exchange YouBit filed for bankruptcy after being hacked.
- 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.
- 12/5 A function targeting cryptocurrency wallet is added to downloader Quant.
- 11/18 Wallet scan of cryptocurrency increased. The prices soared just before it increased.
- 11/7 Coinhive was detected on 2,496 e-commerce websites.
- 10/30 Trend Micro found out malicious apps in Google Play used for mining cryptocurrency in mobile devices.
- 11/6 In Australia, a malicious message was sent out to spread malware infection to mine Bitcoins using mobile phones.
- 10/10 Technique to infect cryptocurrency miner CoinMiner by pretending to install Roboto Condensed font.
- 10/1 Technique to infect cryptocurrency miner CoinMiner.

### Attacks mining cryptocurrency in unauthorized manner
- 11/18 Wallet scan of cryptocurrency increased. The prices soared just before it increased.
- 12/5 A function targeting cryptocurrency wallet is added to downloader Quant.
- 12/15 Russian oil pipeline company, Transneft infected with cryptocurrency miner.
- 12/12 Website of Bitfinex cryptocurrency exchange halted due to DDoS attack.
- 12/15 Attack campaign Zealot targeted the devices on which Apache Struts2 was working and infected cryptocurrency miner mule.
- 12/19 Korean cryptocurrency exchange YouBit filed for bankruptcy after being hacked.
- 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.
- 12/5 A function targeting cryptocurrency wallet is added to downloader Quant.
- 11/18 Wallet scan of cryptocurrency increased. The prices soared just before it increased.
- 10/30 Trend Micro found out malicious apps in Google Play used for mining cryptocurrency in mobile devices.
- 11/6 In Australia, a malicious message was sent out to spread malware infection to mine Bitcoins using mobile phones.
- 10/10 Technique to infect cryptocurrency miner CoinMiner by pretending to install Roboto Condensed font.
- 10/1 Technique to infect cryptocurrency miner CoinMiner.

### Targeting mobile
- 10/30 Trend Micro found out malicious apps in Google Play used for mining cryptocurrency in mobile devices.
- 11/6 In Australia, a malicious message was sent out to spread malware infection to mine Bitcoins using mobile phones.
- 10/10 Technique to infect cryptocurrency miner CoinMiner by pretending to install Roboto Condensed font.
- 10/1 Technique to infect cryptocurrency miner CoinMiner.

### Attacks attempting to steal cryptocurrency from wallets
- 11/18 Wallet scan of cryptocurrency increased. The prices soared just before it increased.
- 12/5 A function targeting cryptocurrency wallet is added to 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.
- 12/5 A function targeting cryptocurrency wallet is added to downloader Quant.
- 11/18 Wallet scan of cryptocurrency increased. The prices soared just before it increased.
- 10/30 Trend Micro found out malicious apps in Google Play used for mining cryptocurrency in mobile devices.
- 11/6 In Australia, a malicious message was sent out to spread malware infection to mine Bitcoins using mobile phones.
- 10/10 Technique to infect cryptocurrency miner CoinMiner by pretending to install Roboto Condensed font.
- 10/1 Technique to infect cryptocurrency miner CoinMiner.
## III. Timeline (2/9)

### [B] Spread of IoT Botnet

- **10/5** Administration panel of around 700 printers of Brother was left unprotected without password. Shipping without protecting it with a password was one reason of exploitation.
- **10/19** A new IoT botnet IoTroop (IoT_reaper) was confirmed around September end and it was spreading to target the vulnerabilities of wireless camera.
- **10/3** Ministry of Internal Affairs and Communications announced “IoT Security Comprehensive Measures” for granting certification mark to highly safe devices such as anti-virus software etc.
- **11/8** IP scanner used in IoT botnet IoTroop was released through backdoor.
- **11/22** Multiple access trials originating in Argentina by Mirai variant were confirmed.
- **11/29** Multiple access trials originating in Columbia, Egypt and Tunisia by Mirai variant were confirmed.

### [C] Targeted attacks on banks

- **10/7** Far Eastern International Bank in Taiwan was hacked and illegal money transfer took place via SWIFT.
- **10/10** Financial institutions in Former Soviet Union were targeted and the technique of increasing cash withdrawal limit illegally for the newly opened illegal account and withdrawing money through cyber attacks.
- **10/17** NIC Asia Bank in Nepal was hacked and money was transferred illegally via SWIFT.
- **10/15** Multiple victims were targeted and illegal money was transferred via SWIFT.
- **11/1** Silence attack targeted the banks in Russia, Malaysia and Armenia. Attacks were made by invading with phishing email to gain adequate information to steal large amount of money.
- **11/21** Cobalt group used phishing mail attack targeting financial institutions in Russia and Turkey. Exploits MS Office vulnerability (CVE-2017-11882).
- **11/20** Multiple critical vulnerabilities in Intel Management Engine (ME)
- **12/18** Malware TelegramRAT spread using Equation Editor vulnerability (CVE-2017-11882)
- **12/20** Pirated version of information stealing malware Loki spread using Equation Editor vulnerability (CVE-2017-11882)

### [A] Countermeasures

- **10/3** Ministry of Internal Affairs and Communications announced “IoT Security Comprehensive Measures” for granting certification mark to highly safe devices such as anti-virus software etc.
- **10/19** A new IoT botnet IoTroop (IoT_reaper) was confirmed around September end and it was spreading to target the vulnerabilities of wireless camera.
- **11/8** IP scanner used in IoT botnet IoTroop was released through backdoor.
- **11/22** Multiple access trials originating in Argentina by Mirai variant were confirmed.
- **11/29** Multiple access trials originating in Columbia, Egypt and Tunisia by Mirai variant were confirmed.
- **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.
- **11/15** MS Office Equation Editor vulnerability (CVE-2017-11882) was published and fixed.
- **11/15** Microsoft to provide patches for Equation Editor vulnerability (CVE-2017-11882) for MS Office 2007 whose service provision ended in October.
- **11/20** Multiple critical vulnerabilities in Intel Management Engine (ME)
- **12/14** 40% of the encryption settings of home wireless LAN were default settings as per IPA survey.
- **10/5** Administration panel of around 700 printers of Brother was left unprotected without password. Shipping without protecting it with a password was one reason of exploitation.
- **12/18** Number of host attacks originating from Japan in November grew 100 times more than October.
- **12/19** About 76% of 1,475 addresses of Lexmark printers were without password as confirmed by Shodan.
- **12/19** Mirai variant targeting the vulnerability of BB router of Logitech and Huawei spread infection.

* Dates indicate either when the events happened, or when the related articles were first appeared.
III. Timeline (3/9)

[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

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

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

© 2018 NTT DATA Corporation
III. Timeline (4/9)

- **Sep**: Early September Ransomware damage in Toshiba memory chips.
- **Oct**: 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.
- **Nov**: 10/9 Attack to manually infect Ransomware BTCWare's new variant via RDP. 10/12 Phishing attack in Ukraine at the same time as the attack by Ransomware BadRabbit. 10/16 Ransomware Tyrant spread in Iran. 10/17 US medical institution group FirstHealth of the Carolinas infected with WannaCry variant. Company network was halted.
- **Dec**: 10/10 Ransomware Spider targeted mainly at areas like Bosnia, Herzegovina etc. 10/13 Ransomware DoubleLocker that exploits Android accessibility service. It has a function to encrypt data and change PIN. 10/24 Ransomware BadRabbit caused damage in Russia, Ukraine etc. 10/24 Attack to infect Ransomware HC7 via RDP. PsExec was used to spread infection across internal networks. 10/25 Aika industry temporarily closed their website since it was used for spreading BadRabbit. 10/29 Ransomware Sage 2.2 variant equipped with Sandbox avoidance and privilege upgrade function.

**Variant**

- **Sep**: 10/11 Sales of Ransomware increased by 2,502% on dark web between 2016 and 2017.
- **Nov**: 10/7 Ransomware GIBON. 11/9 Ransomware LockCrypt targeting servers. Spreads with RDP brute force attack. 11/22 Ransomware qK that infects MS Word template to spread the infection. It was found to be in PoC stage in VirusTotal. 11/26% of Ransomware targeting enterprise users increased to 23% as compared to last year.
- **Dec**: 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". 12/20 Attacker group moved to mining of cryptocurrency using Ransomware VenusLocker.

**Ransomware damage**

- **Sep**: 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.
- **Nov**: 10/12 Phishing attack in Ukraine at the same time as the attack by Ransomware BadRabbit. 10/17 US medical institution group FirstHealth of the Carolinas infected with WannaCry variant. Company network was halted.
- **Dec**: 12/8 Municipal PCs in Nashotah village, Wisconsin, US infected with Ransomware. They paid ransom for decrypting. 12/10 Ransomware Spider targeted mainly at areas like Bosnia, Herzegovina etc. 12/13 Ransomware CryptoMix variant "WORK".
### III. Timeline (5/9)

#### [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.

**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.

**[G] Attacks on critical infrastructure and industrial systems**

- **10/11** DDOS attack on Swedish transportation system.
- **12/14** Malware Triton targeted Industrial control system.
- **12/15** California voter information published on MongoDB was deleted and ransom was demanded.

*Dates indicate either when the events happened, or when the related articles were first appeared.*
III. Timeline (6/9)

**[H] Attacks using DDE (Dynamic Data Exchange)**
- **10/12** A method for executing arbitrary code using DDE was published.
- **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.
- **10/17** Necurs botnet spread Ransomware Locky and Trojan Trickybot. The downloader could gather screen grabs of desktop and also had error reporting functionality.
- **11/8** Microsoft issued advisory against DDE attacks.
- **12/12** Microsoft deactivated DDE feature in Word.

**[I] Attacks using Necurs Botnet**
- **10/20** Necurs botnet spread emails infected with Ransomware Locky using DDE attack.
- **11/23** Necurs botnet spread Ransomware Scarab.

**[J] Attacks by sending email with malicious URL in email body**
- **11/7** Email attack that sent fake emails supposed to be from JCB card.
- **11/29** Email attack that sent fake emails supposed to be from Rakuten card company.
- **12/28** Email attack that sent fake emails supposed to be from Apple support center.

**[K] Business Email Compromise**
- **September** Bank of Tokyo-Mitsubishi UFJ distributed warning messages regarding Business Email Compromise to its enterprise customers.
- **10/5** New Zealand wine growers email account was hacked and invoice mail was sent to different account. It was noticed that usual logo image was different and then damage was avoided.
- **11/8** Trick to cheat the purchaser with discount on down payment in real estate transactions.
- **12/20** Japan Airlines suffered Business Email Compromise from August to September. Losses were a total of around 380 million Yen. A similar email fraud occurred at Skymark Airlines.

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

© 2018 NTT DATA Corporation
III. Timeline (7/9)

[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
- 10/13 Password list attack on Toho Gas member website. Possibility of leakage of personal information of 103 members
- 11/4, 5 Password list attack on Dinos Cecile online shop

[N] Threats to WordPress
- 11/13 Latest variant of malware wp-vcd 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.

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

© 2018 NTT DATA Corporation
III. Timeline (8/9)

- **[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 government stole the confidential documents of NSA via Kaspersky Antivirus products and notified it to US.
  - 10/11 German government announced that there was no evidence that Kaspersky’s security software stole the confidential information of US government
  - 10/12 Kaspersky agreed to share cyber crime threat data with Interpol
  - 10/23 Kaspersky announced independent third party review of the source code for its security products
  - 12/1 UK government agency, NCSC issued warning that Russian based anti-virus software company should not be selected as it poses a risk to national security
  - 12/12 US President signs 2018 National Defense Authorization Act including clause to ban the use of Kaspersky products in federal office
  - 12/18 Kaspersky asked US federal court to overturn the Trump administration ban on its products

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

- ▲: Globally common
- ◆: Vulnerabilities
- ○: Threats
- ●: Cyber attacks/Incidents
- ▲: Domestically in Japan
- ○: Countermeasures
- ●: Governments

© 2018 NTT DATA Corporation
III. Timeline (9/9)

- 9/6 A large amount of information such as sensitive and critical information that was acquired by US Department of Defense was leaked on Amazon S3.
- 9/17 Confidential information of Accenture, Consulting company was leaked on Amazon S3.
- 9/21 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/26 Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3.
- 9/27 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.

- 9/6 A large amount of information such as sensitive and critical information that was acquired by US Department of Defense was leaked on Amazon S3.
- 9/17 Confidential information of Accenture, Consulting company was leaked on Amazon S3.
- 9/21 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/26 Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3.
- 9/27 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.

- 9/6 A large amount of information such as sensitive and critical information that was acquired by US Department of Defense was leaked on Amazon S3.
- 9/17 Confidential information of Accenture, Consulting company was leaked on Amazon S3.
- 9/21 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/26 Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3.
- 9/27 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.

- 9/6 A large amount of information such as sensitive and critical information that was acquired by US Department of Defense was leaked on Amazon S3.
- 9/17 Confidential information of Accenture, Consulting company was leaked on Amazon S3.
- 9/21 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/26 Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3.
- 9/27 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.

- 9/6 A large amount of information such as sensitive and critical information that was acquired by US Department of Defense was leaked on Amazon S3.
- 9/17 Confidential information of Accenture, Consulting company was leaked on Amazon S3.
- 9/21 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/26 Confidential data of INSCOM belonging to US Army and NSA was leaked on Amazon S3.
- 9/27 Medical data of over 47 GB of Patient Home Monitoring, US healthcare company was leaked on Amazon S3.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
- 9/26 Personal information of customers of DJI, drone maker of China was leaked on Amazon S3.
- 9/27 Confidential 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.
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

(*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

(*1-22) 2017/12/12 ADV170021 Microsoft Office Defense in Depth Update | Microsoft Security TechCenter

(*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/


(*2-2) 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

(*2-5) 2018/1/3 NEW PYTHON-BASED CRYPTO-MINER BOTNET FLYING UNDER THE RADAR | F5 Networks