# Table of Contents

1. Executive Summary .................................................................................................................. 3  
2. Topics for 2Q/FY2018 ............................................................................................................. 4  
   2.1. Attacks targeting cryptocurrencies ...................................................................................... 4  
      2.1.1. Attacks targeting systems of cryptocurrency service providers .................................. 4  
      2.1.2. Attacks targeting cryptocurrencies of users of cryptocurrency services on websites .................................................. 4  
      2.1.3. Attacks targeting computing resources of computers ................................................. 5  
      2.1.4. Mobile application measures, including mining processing, and regulations on criminal cryptocurrency transactions .................................................. 7  
   2.2. Ransomware ....................................................................................................................... 7  
   2.3. Attacks involving authentication information ..................................................................... 9  
      2.3.1. Phishing attacks targeting Office 365 .......................................................................... 9  
      2.3.2. Leakage of authentication information ...................................................................... 11  
      2.3.3. Password list attacks ................................................................................................ 11  
      2.3.4. Measures against password list attacks ...................................................................... 12  
   2.4. Attacks using email .......................................................................................................... 12  
      2.4.1. Business email compromise ........................................................................................ 12  
      2.4.2. Threatening email with password ............................................................................... 13  
   2.5. Cyber attacks involving political activities in the U.S. ....................................................... 14  
      2.5.1. Those related to the 2016 U.S. presidential election .................................................. 14  
      2.5.2. Those related to the 2018 midterm election .............................................................. 14  
      2.5.3. Talks between President Trump and President Putin ................................................ 14  
   2.6. Moving to Always on HTTPS ......................................................................................... 15  
   2.7. Discussions on manga piracy websites and blocking ..................................................... 15  
   2.8. Information leakage ......................................................................................................... 16  
   2.9. Botnet ............................................................................................................................... 17  
3. Forecasts for 3Q/FY2018 onward .......................................................................................... 19  
   3.1. Shift from ransomware to attacks targeting cryptocurrencies ........................................ 19  
   3.2. Password list attacks ...................................................................................................... 19  
4. Timeline for 2Q/FY2018 ....................................................................................................... 20  
5. Inquiry Contact ..................................................................................................................... 26  
6. References ............................................................................................................................ 26
1. Executive Summary

With regard to trends in global cyber attacks, attacks targeting cryptocurrencies and ransomware have continued to spread since the last quarter. Attacks targeting cryptocurrencies can be broadly divide into attacks that steal a large amount of cryptocurrencies from the exchange and methods that mine a small amount of cryptocurrencies on a broad scale. The level of security of cryptocurrency exchanges is low when compared to banks that handle legal currencies. Exchanges are expected to take measures against unauthorized access, including segregation of assets to a cold wallet\(^1\) and introduction of multi-signature\(^2\) technology, etc. Users are also expected to exercise due care such as using exchanges certified by public institutions and not to deposit an excessive amount of assets, etc.

Ransomware transformed from types that randomly spread infection such as WannaCry that drew attention in 2017 to those that use more advanced infection and spreading techniques. Cybercriminals tend to target certain companies and organizations that are likely to pay ransoms, attempting to cause ransomware infections. In order to protect assets from ransomware, it is important to ensure basic security measures are in place, including keeping OS and software up-to-date, introducing anti-virus software, and regularly taking backups, etc.

There have been password list attacks on multiple websites, causing damage such as leakage of personal information and fraudulent purchase of goods. Username and password pairs that had previously leaked to the Internet have been used. It seems likely that attacks attempting unauthorized access using the leaked list will continue for the time being. Moreover, as adoption of cloud services by companies becomes more prevalent, damage from phishing attacks that steal accounts for cloud services are increasing. It is therefore important to take measures to prevent unauthorized login, including not reusing passwords and using multi-factor authentication, etc.

---

\(^1\) A wallet completely disconnected from the Internet. It can be used as a measure against unauthorized access from the Internet but with less convenience. The antonym is a hot wallet.

\(^2\) Requiring electronic signatures by multiple private keys for cryptocurrency transactions. Distributed management of private keys improves security because cryptocurrencies cannot be sent even if an attacker obtains a private key.
2. Topics for 2Q/FY2018

2.1. Attacks targeting cryptocurrencies

2.1.1. Attacks targeting systems of cryptocurrency service providers

On September 14, unauthorized access was made to the hot wallet of the cryptocurrency exchange Zaif operated by Tech Bureau and approx. 7 billion yen worth of cryptocurrencies, including Bitcoin, were illegally sent outside [1][2]. The Kinki Local Finance Bureau issued a business improvement order to Tech Bureau to investigate into the cause of the outflow and respond to damage caused to its customers [3].

In addition to this, there have been outflows of cryptocurrencies by unauthorized access in multiple cryptocurrency exchange services (see Table 2). According to a study by Group-IB, the total amount of damages that have been caused to exchanges since 2017 reached $882 million [4].

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline of attack</th>
<th>Amount of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 3</td>
<td>Unauthorized access was made to the cryptocurrency exchange Binance using a large number of API calls. As a result of the attack, the price of the cryptocurrency SYS rose sharply at one point [5].</td>
<td>None</td>
</tr>
<tr>
<td>July 9</td>
<td>Unauthorized access was made to the cryptocurrency exchange Bancor, resulting in outflow of $13.5 million worth of cryptocurrencies. The attacker exploited the wallet used for upgrading smart contracts [6].</td>
<td>$13.5 million</td>
</tr>
<tr>
<td>July 26</td>
<td>Unauthorized access was made to the ICO3 platform KickICO, resulting in outflow of $7.7 million worth of KICK tokens. The attacker exploited the private key for developers to operate smart contracts for KICK token [7].</td>
<td>$7.7 million</td>
</tr>
<tr>
<td>Sep. 1</td>
<td>Unauthorized access was made to the cryptocurrency exchange service Monappy, resulting in outflow of 13 million yen worth of Monacoin cryptocurrencies (all the amount in the hot wallet). The attacker exploited a flaw in the gift code function that occurs under high-load conditions [8].</td>
<td>13 million yen</td>
</tr>
</tbody>
</table>

2.1.2. Attacks targeting cryptocurrencies of users of cryptocurrency services on websites

Users of cryptocurrency services log in to exchanges or online wallet website when making cryptocurrency transactions (purchasing or sending cryptocurrencies). Attackers deliver malware to user PCs to replace destination address with the attackers’ accounts as shown in Table 2, or steal cryptocurrencies by establishing phishing sites, such as that of the online wallet Trezor as shown in Figure 1, to illegally obtain authentication information.

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline of attack</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 13</td>
<td>Qihoo 360 discovered malware that stole cryptocurrencies. This malware replaced Bitcoin addresses copied to users' clipboards with addresses owned by the attacker to send Bitcoins to the attacker’s wallet. Over 300,000 PCs were found to be infected worldwide [9].</td>
<td>300,000 PCs</td>
</tr>
<tr>
<td>July 1</td>
<td>The online wallet service Trezor announced that it had detected phishing attacks (Figure 1) targeting users of the said service. These attacks used DNS poisoning and BGP hijacking to direct users to malicious websites [10][11].</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 1: List of attacks targeting systems of cryptocurrency service providers

Table 2: List of attacks targeting cryptocurrencies of users of cryptocurrency services on websites

---

3 A method of raising funds by issuing Initial Coin Offering cryptocurrencies.
2.1.3. Attacks targeting computing resources of computers

Cryptocurrencies, such as Bitcoin, etc., can be acquired through mining. Attackers attempt to gain profits by delivering malware to a number of computers and using the malware to conduct large-scale mining. It is characterized by the fact that computers that do not directly use cryptocurrencies are also targeted.

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline of attack</th>
<th>Number of units damaged</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 3</td>
<td>The security company Malwarebytes reported of an attack known as “drive-by mining” (Figure 2) which caused cryptocurrency mining to be conducted on the background when certain websites were accessed. It used a method of fraudulently embedding obfuscated codes with a shortcut link to Coinhive, a service to mine cryptocurrency, in websites, including CMS websites, etc. [12]</td>
<td>N.A.</td>
</tr>
<tr>
<td>July 26</td>
<td>The security company Kaspersky reported of the malware known as “PowerGhost” which mined cryptocurrencies. It was a type of malware that used PowerShell and spread using the attacking tool EternalBlue. PowerGhost infections were found mainly in India, Brazil, Colombia, and Turkey [13] [14]. (Figure 3)</td>
<td>N.A.</td>
</tr>
<tr>
<td>Aug. 14</td>
<td>The security company Symantec reported of an attack that exploited MikroTik routers to mine cryptocurrency. According to its investigation, 157,000 routers were infected worldwide. The attacker exploited the vulnerability CVE-2018-14847, which allowed bypassing router authentication, and displayed an error page embedded with a mining program to users accessed through infected routers to cause cryptocurrency mining [15] [16].</td>
<td>157,000 routers</td>
</tr>
</tbody>
</table>

---

Figure 1: Phishing site of Trezor [11]

4 The act of solving mathematical problems to generate new blocks in the cryptocurrency network. Cryptocurrencies can be acquired as a reward for solving the problems.
Figure 2: Attack causing cryptocurrency mining by drive-by mining [12]

Figure 3: Regions infected by PowerGhost [14]
2.1.4. Mobile application measures, including mining processing, and regulations on criminal cryptocurrency transactions

In response to the problem that mining processing was included in mobile applications without permission, official application stores have been removing mobile applications with the mining function. In addition, when compared to legal currencies controlled by central banks, cryptocurrencies are highly anonymous and therefore difficult to trace when used in crimes. The government and industry associations have been discussing measures to improve transparency of cryptocurrency transactions.

Table 4: List of regulations on mining and cryptocurrencies

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 30</td>
<td>Google followed Apple in prohibiting cryptocurrency mining in their mobile applications [17].</td>
</tr>
<tr>
<td>Aug. 29</td>
<td>The National Police Agency made a decision to introduce a system to effectively identify cryptocurrency transaction histories. The purpose was to make use of it in investigation of crimes involving cryptocurrencies by overviewing transaction flows [18].</td>
</tr>
<tr>
<td>Sep. 12</td>
<td>At the 5th meeting of the “Study Group on the Virtual Currency Exchange Services” held by the Financial Services Agency, the Japan Virtual Currency Exchange Association presented a proposal for self-regulation of cryptocurrency exchange business [19]. It included setting an upper limit on the leverage magnification factor and prohibiting anonymous currencies, etc. Members of the said Association consist of major domestic cryptocurrency business operators, including Money Partners and bitFlyer, etc.</td>
</tr>
</tbody>
</table>

2.2. Ransomware

The targets of cybercriminals are said to have shifted from obtaining ransoms using ransomware to obtaining cryptocurrencies. In terms of the number of cases and amount of damage, however, ransomware remains to be a significant threat. According to Trend Micro, the number of cases of ransomware detected in the first half of 2018 increased by 3% from the second half of 2017 to approx. 380,000 [20]. According to a study by the security company Sophos and Neutrino, the amount of damage caused by the ransomware SamSam during the period from January 2016 to July 2018 reached $5.9 million [21].

Wide-ranging ransomware infection routes include via emails and websites and direct delivery through network, etc. It is therefore important to take measures such as regularly taking backup of files and systems, keeping software up-to-date, and updating security software, etc. [22]

Table 5: List of damage caused by ransomware

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
<th>Amount of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 5</td>
<td>Kaspersky discovered a malware that changed its behavior according to the environment. When the “Bitcoin” folder exists, it acted as ransomware and encrypted files; Otherwise it acted as a coin miner and mined cryptocurrencies [23].</td>
<td>-</td>
</tr>
<tr>
<td>July 25</td>
<td>The US site of the Chinese maritime shipping company COSCO was infected by ransomware. Ransomware infection affected internal email systems and telephone systems [24].</td>
<td>N.A.</td>
</tr>
<tr>
<td>Aug. 1</td>
<td>The city of Atlanta announced that the damage caused by the ransomware infection case that took place in the city in March was $17 million [25].</td>
<td>$17 million</td>
</tr>
<tr>
<td>Aug. 3</td>
<td>The Taiwanese semiconductor manufacturer TSMC (Taiwan Semiconductor Manufacturing Company) was infected with ransomware. The ransomware, a variant of WannaCry, infected to devices in the plant during software installation [26]. TSMC manufactures IC chips for iPhones. TSMC announced that delay in shipping and additional costs due to the ransomware infection would cause the impacts of a 3%-decrease in sales and a 1%-decrease in profits [27].</td>
<td>Impacts of a 3%-decrease in sales and a 1%-decrease in profits</td>
</tr>
<tr>
<td>Aug. 13</td>
<td>Kaspersky discovered a new variant of the ransomware KeyPass. It was characterized by the fact that the attacker could change the content of the threatening letter and encryption target files after the infection [28] (Figure 4).</td>
<td>-</td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>July 9</td>
<td>The ransomware GandCrab was updated to version 4 on July 9 and to version 5 on September 26. GandCrab is a Malware-as-a-Service (MaaS) platform introduced in January 2018 and has frequently been used because it is inexpensive. Version 4 adopted the Salsa20 stream encryption cipher as the encryption method and the encryption operation became faster than that based on RSA-2048 [29]. Version 5 was created to exploit the zero-day vulnerability CVE-2018-8440 in Windows Task Scheduler released in August [30]. (Figure 5)</td>
<td></td>
</tr>
<tr>
<td>Sep. 10</td>
<td>Trend Micro discovered the ransomware PyLocky designed to avoid detection by machine learning. Two types of installers (PyInstaller and Inno Setup Installer) were combined to make static analysis by security software difficult [31].</td>
<td></td>
</tr>
</tbody>
</table>

---

![GUI screen of KeyPass](image)

**Figure 4:** GUI screen of KeyPass [28]
2.3. Attacks involving authentication information

2.3.1. Phishing attacks targeting Office 365

Phishing attacks stealing account information for cloud email services prevailed. The Microsoft Office 365 services was targeted in particular. According to a study by Trend Micro, nine cases of damage were found in educational institutions and companies in the first half of 2018 [33].

When compared to on-premise email servers within the company, the login screen for cloud services is exposed to the Internet and can be attacked by anyone. According to a study on European companies conducted by the security company Bitglass, the share of Office 365 in cloud services was 43% in 2016 and 65% in 2018 [34]. In addition, Microsoft is also expected to promote migration from on-premise to Office 365 [35]. As companies using Office 365 are increasing, Office 365 is becoming an attractive target for attackers.
Table 6: List of phishing attacks targeting Office 365

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Number of cases of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 27</td>
<td>In response to the leakage of approx. 12,000 personal information occurred in six national/public/private universities due to phishing emails, the Ministry of Education, Culture, Sports, Science and Technology alerted universities across the country to strengthen measures. Six universities that suffered damage were Yokohama City University, Shimane University, Toyama Prefectural University, Okinawa Prefectural College of Nursing, Hirosaki University, and Ritsumeikan University. All of them were using Office 365 [36].</td>
<td>12,000 personal information</td>
</tr>
<tr>
<td>Q2/FY2018</td>
<td>According to the report “Phishers’ Favorites” by the security company Vade Secure, the most frequently targeted domain was Microsoft at 56.6% [37].</td>
<td>-</td>
</tr>
<tr>
<td>Aug. 16</td>
<td>The security company Avanan detected the phishing attack “PhishPoint” targeting Office 365 users. The attacker sent emails containing a link to a Share Point document to targets. The document contained a malicious URL disguised as a link to a OneDrive file (Figure 6). Clicking the URL would direct users to the fake Office 365 login screen (Figure 7) to steal their authentication information [38].</td>
<td>Estimated to have affected 10% of Office 365 users</td>
</tr>
</tbody>
</table>

Figure 6: Share Point file containing a malicious URL link [38]
2.3.2. Leakage of authentication information

On September 7, the Nikkei Business reported that lists containing 1.6 billion email addresses and passwords of employees of Japanese companies had been leaked to the Internet [39]. The leaked authentication information was not directly leaked from the companies concerned nor was newly leaked, but was gathered from the authentication information leaked in the past, which was registered on external websites [40] [41].

2.3.3. Password list attacks

“Password list attacks” that use username and password pairs leaked to the Internet to attempt unauthorized logins were conducted against multiple websites in Japan. The leakage of 1.6 billion passwords might activate those kinds of attacks.

Table 7: List of password list attacks

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
<th>Number of cases of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>July to Aug.</td>
<td>Unauthorized access was made to the Docomo Online Shop and iPhone X units were fraudulently purchased. The number of iPhone X units fraudulently purchased was estimated to be approx. 1,000 [42].</td>
<td>Approx. 1,000 units</td>
</tr>
<tr>
<td>Aug. 15</td>
<td>Unauthorized access was made to eoID, which is the account for using various services provided by K-Opticom, including eo and mineo, etc. Personal information of 7,131 customers might have been viewed [43].</td>
<td>7,131 personal information</td>
</tr>
<tr>
<td>Sep. 10</td>
<td>Unauthorized access was made to the “smartWAON Website” operated by Aeon Marketing, resulting in transfer of WAON points of 52 customers to other cards [44].</td>
<td>WAON points of 52 customers</td>
</tr>
</tbody>
</table>
2.3.4. Measures against password list attacks

- According to a study conducted by Trend Micro in 2017, 85.2% of users reused their passwords in multiple services [45]. Reusing the same password in multiple services allows unauthorized login to other services when a password for a service is leaked. Not reusing passwords and using different passwords for each service can limit damage when, by any chance, a password is leaked [46].

- Multi-factor authentication is an authentication method that combines at least two factors of authentication, namely biological information, knowledge information, and possession information. Using multi-factor authentication makes unauthorized login difficult when compared to password (knowledge information) only authentication [47]. The following combinations have been used.

  (Example 1) Password (knowledge information) and fingerprint (biological information)
  (Example 2) Password (knowledge information) and hardware token (possession information)

- Depending on the types of cloud services, an email is sent to the user to notify of his/her login. This enables early detection of successful unauthorized login attempts by the attacker. Additionally, some cloud services prevent unauthorized logins by requiring additional authentication (risk based authentication) a login attempt is made from locations or browsers that are different from those that are normally used.

2.4. Attacks using email

2.4.1. Business email compromise

Business email compromise (BEC) is a crime in which the attacker impersonates a relevant party and communicates with the company’s staff through emails to deceive them to transfer money to the fake account prepared by the attacker. The cases have previously occurred mainly abroad (in English), but now business compromise emails are also being sent to Japan (in Japanese). Having the company's finance department understand fraud schemes and establishing a system for checking by multiple persons can reduce damage from compromise.

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
<th>Number of cases and amount of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 12</td>
<td>According to the investigation by FBI, there had been 78,000 cases of BEC with damage of $12.5 billion for the period from October 2013 to May 2018 [48].</td>
<td>78,000 cases, $12.5 billion</td>
</tr>
<tr>
<td>Aug. 15</td>
<td>According to a questionnaire survey conducted by Trend Micro, 39% of companies had received fraud emails and 5% of companies had actually transferred money and suffered damage [49].</td>
<td>5% of companies actually transferred money</td>
</tr>
<tr>
<td>Aug. 27</td>
<td>IPA alerted that it had found a case of attack using Japanese [50].</td>
<td>-</td>
</tr>
<tr>
<td>Sep. 5</td>
<td>The security company Antuit announced that it had observed intelligence activities regarding fraud that had taken advantage of the Tokyo Olympic Games in 2020 [51].</td>
<td>-</td>
</tr>
</tbody>
</table>
2.4.2. Extortion email with password

JP CERT/CC alerted that extortion emails demanding Bitcoin payments had been sent since around July 21. The email claimed that “an image of the receiver viewing pornographic websites was secretly recorded using the web-camera” and he/she “must pay money to prevent it from being disclosed” (Figure 9). It was characterized by the fact that the password that the receiver had actually used was written in the email body to convince as if it was true [52]. According to a study by Trend Micro, as of October 1, a total of 3.4 BTC (equivalent to 2.5 million yen) had been paid in 46 cases [53].

Figure 8: Business email compromise using Japanese [50]

Figure 9: Extortion email demanding Bitcoin payment [53]
2.5. Cyber attacks involving political activities in the U.S.

2.5.1. Those related to the 2016 U.S. presidential election

Since the “Russian interference” in which the Russian government is suspected to have interfered in the U.S. presidential election, concerns over cyber attacks from abroad have been growing in the U.S.

Table 9: Events related to the 2016 U.S. presidential election

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 13</td>
<td>In relation to the presidential election, the U.S. authorities have charged 12 Russian intelligence officers with domestic computer intrusion. They were said to have used Bitcoin, which has high anonymity, for purchasing servers, registering domains, and other hacking related payments [54].</td>
</tr>
<tr>
<td>Aug. 1</td>
<td>The U.S. government made a statement that it would create a new department within the government to prepare for large-scale cyber attacks against important public infrastructure, including financing, electricity, and communications [55].</td>
</tr>
<tr>
<td>Sep. 21</td>
<td>The U.S. government published the “National Cyber Strategy”, which compiled national security policies to protect U.S. citizens from threats in cyberspace. It listed four countries, namely Russia, China, Iran, and North Korea, as “adversaries” and criticized that “(these four countries) use cyber tools to undermine our economy and democracy, steal our intellectual property” [56].</td>
</tr>
</tbody>
</table>

2.5.2. Those related to the 2018 midterm election

On July 19, Microsoft announced that it stopped attempts to launch cyber attacks against three midterm election candidates. The attacker used the phishing tactics similar to “2.3.1 Phishing attacks targeting Office 365”, attempting to steal authentication information of candidates’ campaign staff by creating an authentication page disguised as Microsoft’s domain [57]. On August 21, Microsoft announced again that it stopped attempted attacks by the cyber attack group APT28 (Fancy Bear) [58].

2.5.3. Talks between President Trump and President Putin

On July 16, President Trump and President Putin talks in Helsinki. From July 12, just before the talks, cyber attacks against Finland have sharply increased (Figure 10). These attacks originated from China and used SSH (TCP 22) and SMB (TCP 445) ports [59].

![Attacks against Finland](image)

**Figure 10: Sharp increase in attack traffic directed toward Finland [59]**
2.6 Moving to Always on HTTPS

Encrypting the entire website, instead of encrypting only some pages of the website that contain sensitive information, is called “Always on HTTPS (SSL)”. For the following reasons, moving to Always on HTTPS is accelerating [60].

- Masquerading and wiretapping can be prevented, thereby improving safety for website visitors
- Access analysis accuracy can be improved, thereby benefiting website administrators
- HTTPS is practically required for using the next generation protocol HTTP/2 to benefit from improved speed

However, moving to Always on HTTPS is seemed to be delayed for websites of Japanese ministries/agencies and local governments. As of October 1, the websites of the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications have not been moved to Always on HTTPS. As of early June, 37.4% of local governments’ websites have moved to Always on HTTPS [61]. When accessing websites that have not moved to Always on HTTPS, an alarm display, as shown in Figure 11, appears in the banner portion of the browser.

### Table 10: Events concerning Always on HTTPS

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 24</td>
<td>Version 68 of Google Chrome was released. From this version onward, a logo “Not secure” (unprotected communication) is displayed in the banner of HTTP-based websites [62].</td>
</tr>
<tr>
<td>Aug. 24</td>
<td>According to a study by a security researcher, majority of Alexa’s top 1 million websites have moved to HTTPS [63].</td>
</tr>
</tbody>
</table>

![Figure 11: Alarm display in the banner of HTTP-based websites [62]](image)

2.7 Discussions on manga piracy websites and blocking

Pirated manga websites that post images of popular manga works without permission have been an issue. “Manga-Mura” in particular had many users, with the number of monthly users exceeding tens of millions. The Content Overseas Distribution Association estimated the amount of damage caused by “Manga-Mura” to be approx. 300 billion yen [64]. “Manga-Mura” was closed in late April and is no longer accessible, but preventing similar websites from appearing is difficult. A measure being discussed is “website blocking”.

Website blocking is a mechanism in which Internet service providers (ISPs) automatically detect users viewing the websites concerned and block them (Figure 12). Implementing website blocking allows ISPs to identify tastes and interests, etc. of users, which may cause privacy issues. How should disadvantages caused by copyright infringement and disadvantages caused by infringement of secrecy of communications of general users be adjusted is being discussed [65].

---

5 Alexa Internet. It is an Internet-related company that collects data on website usage.
Table 11: Events related to piracy websites

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
</tr>
</thead>
</table>
| Apr. 13   | The Japanese government held a meeting of the Ministerial Meeting Concerning Measures Against Crime, Intellectual Property Strategic Headquarter and decided on measures against manga piracy websites [66].  
As a temporary emergency measure until laws are established, it is considered appropriate to implement blocking exclusively against three websites, namely “Manga-Mura”, “Anitube”, and “Miomio”, and other equivalent websites as voluntary efforts of private business operators. |
| Apr. 23   | Three companies, namely NTT Communications, NTT Docomo, and NTT Plala, announced that they would implement blocking against three manga piracy websites, including “Manga-Mura”, etc. [67]. |
| June to Oct. | The Japanese government held meetings of the “Study Group on Measures against Internet Piracy” and discussed measures against piracy websites. The 9th meeting was held on October 15, but the planned “Interim Summary” was not completed and further meetings were postponed indefinitely [68]. |

Figure 12: Mechanism of website blocking [69]

2.8. Information leakage

Large-scale information leakage due to unauthorized access repeatedly occurred on overseas websites. Moreover, there had been unintended data disclosure due to inadequate access privileges in online storage such as AWS S3, etc. and database such as MongoDB, etc.

Table 12: List of information leakage incidents

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
<th>Number of cases of damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 18</td>
<td>Leakage of customers’ personal information occurred on the Adidas U.S. Website. Millions of customers were affected, and the information leaked included their contact information, names, and encryption passwords [70].</td>
<td>Millions of personal information</td>
</tr>
<tr>
<td>July 11</td>
<td>Leakage of users’ personal information occurred in Timehop application. Approx. 21 million users were affected, and the information leaked included their names, email addresses, and birthdays. The attacker obtained authentication information of the cloud environment of the said company and broke into the system [71].</td>
<td>21 million personal information</td>
</tr>
<tr>
<td>July 19</td>
<td>Leakage of users’ personal information occurred in Reddit. The attacker accessed database backup data of 2007 and earlier and obtained email addresses and password hashes. Reddit has been using multi-factor authentication, but the attacker wiretapped SMS and broke through multi-factor authentication [72].</td>
<td>All users registered in May 2007 and earlier</td>
</tr>
</tbody>
</table>
July 20  The Singapore government announced that patient information had been leaked from the medical group SingHealth due to unauthorized access. Approx. 1.5 million patients were affected, and the information leaked included their names, sex, and addresses. The Prime Minister of Singapore was also included, and the government said that it was a highly advanced attack targeting certain targets [73].

Aug. 21 to Sep. 5 There had been an attack against the British Airways website, stealing user inputs on mobile applications. Approx. 380,000 persons were affected, and the information stolen included names and credit card information entered on the website [74]. The security company RiskIQ pointed out that it was deemed to have been committed by the cybercrime group Magecart because of the similarity with the information leakage case occurred in Ticketmaster in June [75].

2.9. Botnet

While connecting various devices and home electric appliances to the Internet improves the convenience, cases where vulnerable IoT devices are invaded and added to Botnet are increasing. Once IT devices are added to Botnet, they can unintentionally assist cyber attacks and crimes. For IoT devices connected to the Internet, measures such as changing the default password of administrator’s account to a strong password, regularly updating software, and not opening unnecessary ports, etc. should be taken.

<table>
<thead>
<tr>
<th>Date</th>
<th>Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 4</td>
<td>According to the Ministry of Internal Affairs and Communications, vulnerabilities such as inadequate password setting, etc. were found in 150 IoT devices already deployed in important infrastructure [76].</td>
</tr>
<tr>
<td>July 20</td>
<td>According to a study by the security company Avast, 68% of users had not changed the default authentication information of routers and 64% had not updated the firmware [77].</td>
</tr>
<tr>
<td>July 23</td>
<td>The security company Fortinet alerted that the Botnet Hide 'N Seek had been spreading, targeting home electric appliances. The total number of IoT devices is estimated to reach 20.4 billion by 2020, suggesting an increased likelihood of vulnerabilities. [78].</td>
</tr>
</tbody>
</table>

Figure 13: Malicious JavaScript code inserted in the British Airways website [75]
July 23  |  Trend Micro alerted the spread of a variant of the malware Satori that infects IoT devices to form Botnet. A sharp increase in traffic scanning TCP 5555, which is the Android debug port, had just been detected (Figure 14) [79].

Sep. 9   |  The security company PaloAlto reported that it had found variants of the Botnets Mirai and Gafgyt. A variant of Mirai exploited the vulnerability (CVE-2017-5638) of Apache Struts. It was the vulnerability exploited in the case of information leakage occurred in the U.S. consumer credit information company Equifax in 2017. A variant of Gafgyt exploited the vulnerability (CVE-2018-9866) of the firewall product SonicWall released in August [80].

![Figure 14: Sharp increase in traffic scanning TCP 5555 due to a variant of the malware Satori [79]](image-url)
3. Forecasts for 3Q/FY2018 onward

NTTDATA-CERT forecasts the trends in cyber attacks for 3Q/FY2018 onward as follows.

3.1. Shift from ransomware to attacks targeting cryptocurrencies

Attacks targeting money will continue to shift from ransomware to attacks targeting cryptocurrencies. However, attacks involving coin miners, which cause cryptocurrency mining, will relatively decrease, while attacks that directly steal cryptocurrencies from exchanges and users will increase. The reasons are the following two:

- To mine major cryptocurrencies, you need specialized hardware. Using general purpose machines (PCs) for mining cannot provide sufficient profits.
- The prices of minor cryptocurrencies tend to fluctuate, and profits cannot be gained by mining.

From the reasons given above, crimes targeting new exchanges with weak security and deceiving users to transfer money is likely to increase.

3.2. Password list attacks

The effectiveness of password list attacks had been proven by past cases of successful unauthorized logins. In many services, email addresses are used as account names, and cases of leakage of email addresses to the Internet also occurring continually. There is a concern over large-scale password list attacks occurring from combining the leaked lists.
4. Timeline for 2Q/FY2018

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.


[A] Cryptocurrencies

Mining malware

July 3: Malwarebytes reported of a cryptocurrency mining attack that used drive-by mining.

July 6: Sophos reported that Polis Bay caused cryptocurrency mining again using Coinhive and CryptoLoot.

July 20: Ransomware "Jigsaw" turned into a malware to obtain Bitcoin.

July 25: An unemployed 24 years old man who had used Coinhive for malicious purposes was convicted.

Aug. 14: Symantec reported of an attack that exploited MikroTik routers to cause cryptocurrency mining.

Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated.


Aug. 23: Kaspersky observed the attack campaign "AppleJea".

Aug. 29: An attack using the mining malware "CNRig" was observed.


Aug. 29: An attack using the mining malware "CNRig" was observed.

Aug. 24: The National Police Agency made a decision to introduce a system to effectively identify cryptocurrency transaction histories.

Aug. 2: It was discovered that over 200,000 MikroTik routers were infected with malware.

July 10: GooglePlay store removed mining applications.


July 30: GooglePlay store removed mining applications.


Aug. 1: Unauthorized access to Monappy, resulting in outflow of 13 million yen worth cryptocurrencies.

Aug. 29: The National Police Agency made a decision to introduce a system to effectively identify cryptocurrency transaction histories.

Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated.

July 3: Malwarebytes reported of a cryptocurrency mining attack that used drive-by mining.

July 20: Ransomware "Jigsaw" turned into a malware to obtain Bitcoin.

July 20: Ransomware "Jigsaw" turned into a malware to obtain Bitcoin.


Aug. 29: An attack using the mining malware "CNRig" was observed.

Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated.

Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated.

Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated.
* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.
1Q Aug. Sep.

[D] IoT devices

- July 3: The Ministry of Internal Affairs and Communications established an investigation system equivalent to Shodan.
- Aug 9: JPCERT/CC published the “First Step in Security for Deploying Industrial IoT in Factories”.
- Aug 21: Avast found that over 49,000 MQTT servers were open to the Internet.
- Aug 6: The U.S. Department of Energy announced that the cyber attack training “Liberty Eclipse” against power network had been conducted.
- Aug 8: The Ministry of Internal Affairs and Communications announced that the security level of IoT devices in 150 infrastructure facilities nationwide was insufficient.

Attacks targeting routers

- Aug 24: The U.S. Department of Homeland Security announced that a Russian APT group had penetrated in important infrastructure in the U.S., including electric power companies, etc.
- Aug 9: Variant of Gafgyt.
- Aug 9: Variant of Mirai.
- Aug 26: VpFilter function was added.
- Aug 21: Avast found that over 49,000 MQTT servers were open to the Internet.
- Aug 21: The Maas5 “Black Rose Lucy”, which provided infrastructure for bot targeting Android devices, was found.
- Aug 28: The number of IoT botnets “Hide and Seek” consisting of Android devices exceeded 90,000.

[E] Attacks targeting important infrastructure

- Aug 27: J.CSIP found targeted attack emails targeting suppliers of plant equipment and parts in the 2Q.
- Aug 2: Variant of Satori.
- Sep 9: Variant of Gafgyt.
- Sep 9: Variant of Mirai.
- Sep 26: VpFilter function was added.
- Sep 21: The Ministry of Internal Affairs and Communications announced that the security level of IoT devices in 150 infrastructure facilities nationwide was insufficient.
- Sep 23: Cyber attacks took place in the Port of Barcelona, affecting some servers and systems.
- Sep 26: The number of IoT botnets “Hide and Seek” consisting of Android devices exceeded 90,000.

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.

▲: Worldwide ▲: Limited to some overseas regions ▲: Limited to Japan
V: Vulnerability ▲: Threat ▲: Cyber attack/incident ▲: Measure ▲: Government effort
▲: Vulnerability ▲: Threat ▲: Cyber attack/incident ▲: Measure ▲: Government effort

[F] Password list attacks

- July 5: Dinos Cecil; Possible leakage of 460 "personal information"
- Aug. 13: NTT Docomo; Substantial damage from fraudulent purchase of 1,000 units of "iPhone X"
- Aug. 15: K-Quitcom; Possible leakage of 7,131 "personal information"
- Aug. 24: Aplus Financial; Possible leakage of 945 "personal information"
- Aug. 28: Mimecast announced that the number of BEC attacks detected increased by 80% in the last quarter

[G] Phishing

- July 1: Vade Security announced that the most commonly targeted brand for phishing purposes in North America in 2Q/2018 was Microsoft
- July 1: There had been a case where accessing the correct URL resulted in access to a fake website in online wallet services of Trezor
- July 9: There had been a spread of SMS disguised as notifications from parcel delivery services, causing installation of malicious applications in Android devices
- Aug. 9: There had been a spread of the technique of directing users to fake websites to prompt them to enter mobile phone numbers and "authentication codes" was discovered
- Aug. 16: Avanan detected the phishing attack "PhishPoint" targeting Office 365 users

[H] Attacks using email

- Aug. 2: Suspicious emails written in English demanding cryptocurrencies were widely circulated
- Aug. 4: Four Japanese were arrested for soliciting an agriculture-related company in the U.S. to transfer 70 million yen
- Aug. 8: An attack campaign using emails attached with Firefox.exe with the extension ".iqy" was observed. The victims would eventually be infected with the banking malware "Ursnif"
- Aug. 10: Attack campaign using emails attached with Firefox.exe with the extension "iqy" was observed. The victims would eventually be infected with the banking malware "Ursnif"
- Aug. 16: Avanan detected the phishing attack "PhishPoint" targeting Office 365 users
- Aug. 17: Trend Micro released the study results that 39% of companies had received fraud emails and 5% of companies had actually transferred money and suffered damage
- Sep. 10: Antuit observed intelligence activities regarding fraud that had taken advantage of the Tokyo Olympic Games in 2020
- Sep. 13: The U.S. Attorney's Office sentenced the Nigerian accused to 5 years in prison. The total amount of damage suffered exceeded $25 million

- Aug. 24: Sudden increase of unsolicited emails and SNS disguised as absence/shipment notifications from Sagawa Express
- Aug. 27: IPA released the report "Business Mail Compromise (BEC) related Cases and Reminders (Follow-up)"
- Sep. 5: Antuit observed intelligence activities regarding fraud that had taken advantage of the Tokyo Olympic Games in 2020
- Sep. 7: Nikkei Business Online reported that 1.6 billion passwords had been leaked to the Internet
- Sep. 10: Lawson; Alerted of list-based attacks
- Sep. 8: Lawson; Alerted of list-based attacks
- Sep. 10: Lawson; Forsibly reset passwords of all members due to list-based attacks
- Sep. 12: NTT Docomo; 35,000 possible cases of fraudulent use of "dPoints"
- Sep. 13: Tokyo Metropolitan Police Department arrested a Nigerian suspect for soliciting a U.S. company to transfer approx. 100 million yen
- Sep. 13: The U.S. Attorney's Office sentenced the Nigerian accused to 5 years in prison. The total amount of damage suffered exceeded $25 million

- Aug. 15: Trend Micro released the study results that 39% of companies had received fraud emails and 5% of companies had actually transferred money and suffered damage

- Aug. 13: NTT Docomo; Substantial damage from fraudulent purchase of 1,000 units of "iPhone X"
- Aug. 18: Lawson; Alerted of list-based attacks
- Aug. 18: Avanan detected the phishing attack "PhishPoint" targeting Office 365 users
- Aug. 24: Sudden increase of unsolicited emails and SNS disguised as absence/shipment notifications from Sagawa Express
- Aug. 27: IPA released the report "Business Mail Compromise (BEC) related Cases and Reminders (Follow-up)"

- Aug. 24: Shikoku Electric Power; Exploitation of 149 customers' "Yonden Points"
- Aug. 28: Mimecast announced that the number of BEC attacks detected increased by 80% in the last quarter

- Aug. 27: IPA released the report "Business Mail Compromise (BEC) related Cases and Reminders (Follow-up)"
- Aug. 28: Mimecast announced that the number of BEC attacks detected increased by 80% in the last quarter

- Aug. 8: An attack campaign using emails attached with Firefox.exe with the extension "iqy" was observed. The victims would eventually be infected with the banking malware "Ursnif"

* Dates listed in timeline may not be the date of the occurrence of the event but instead the date they were posted in articles.
Information leakage

Unauthorized access

- July 2: Fortnum & Mason; Possible leakage of 23,000 “personal information”
- July 11: Timshop; Leakage of 21 million “personal information”
- July 12: “Confidential documents” of the U.S. armed forces on Unmanned Aerial Vehicle training had been leaked and sold on the Internet
- July 19: Reddit; Leakage of “personal information”
- July 31: UnityPoint Health; Possible leakage of 1.4 million patients’ “personal information” due to phishing attack
- August 2: Kondo Yuki; Leakage of “customer credit card information”
- August 4: Family Orbit; Leakage of hundreds of “photographs of children”
- August 6: NHS Digital; Leakage of 150,000 patients’ “personal information”
- August 11: Veeam; Approx. 445 million “personal information” stored in MongoDB had been disclosed
- August 15: Babahol; Disclosure of “e-labor” 105,000 “personal information” stored in MongoDB had been disclosed
- August 23: Air Canada; Possible leakage of 20,000 “personal information” from a mobile application
- August 26: Eir; Leakage of 37,000 “personal information” due to laptops been stolen. HDDs were not encrypted
- September 5: Activity monitoring application “mSpy”; Hundreds of “personal information”, including encryption keys, stored in database had been disclosed
- September 6: Family Orbit; Leakage of hundreds of “photographs of children”
- September 6: British Airways; Leakage of 380,000 “personal information”
- August 11: Veeam; Approx. 445 million “personal information” stored in MongoDB had been disclosed
- August 24: Cheddars Scratch Kitchen; Leakage of 977,000 “credit card information”. It was found to have been sold on the Dark Web
- August 24: T-Mobile; Possible leakage of 5 million “personal information”
- August 28: Cryptocurrency investment site Atlas; Leakage of 364,000 “personal information”. No cryptocurrencies were stolen
- August 29: Air Canada; Possible leakage of 20,000 “personal information” from a mobile application
- August 28: Cryptocurrency investment site Atlas; Leakage of 264,000 “personal information”. No cryptocurrencies were stolen
- August 30: Huazhu Hotels Group; 500 million “personal information” were found to have been sold on the Dark Web. The leakage route was unknown
- August 24: T-Mobile; Possible leakage of 2 million “personal information”
5. Inquiry Contact

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department
nttda-cert@kits.nttdata.co.jp

6. References


[8] Monappy, "MonappyにおけるMonacoinの不正出金につきまして," 29 7 2018. [Online]. Available: https://medium.com/@IndieSquare/monappy%E3%81%AB%E3%81%8B%E3%81%91%E3%81%88%8Bmonacoin%E3%81%AE%E4%B8%BD%E6%AD%A3%E5%87%BA%E9%87%91%E3%81%AB%E3%81%A4%E3%81%8D%E3%81%BE%E3%81%97%E3%81%A6-bdb1179e2bb9.


年上半期セキュリティラウンドアップ

大学で被害が予測、移行促進を強硬へ?

の偽メールに注意喚起、万ドル以上に、警戒弱まる深夜や早朝を狙って攻撃発表


