

# A Certain Emotet Campaign

Impact on Japan

A community of personal researchers tracking spam “BARAMAKI”

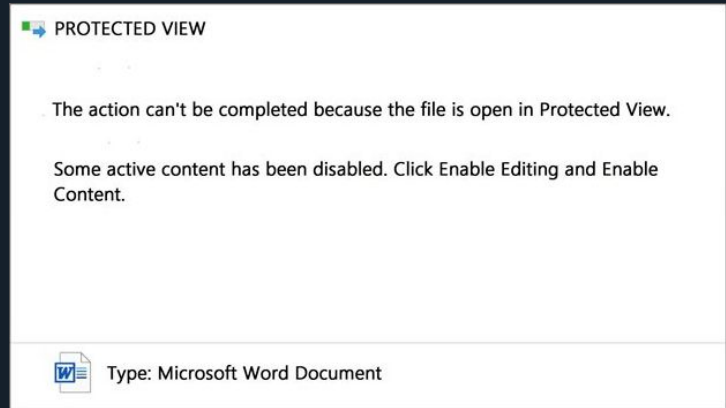
Ken Sajo : JPCERT Coordination Center [@bomccss](#)

Shuhei Sasada : Cyber Defense Institute, Inc. [@sugimu\\_sec](#)

# Agenda

1. Introduction
2. What is Emotet?
3. Impact of Emotet on Japan
4. Damage reduction measures
5. Emotet Campaign Analysis
6. Countermeasures
7. Summary

# 1. Introduction



# 1.1. Who we are

We are an individual member of the spam tracking community called "BARAMAKI".

This community is consist of CSIRT members at user side and security researchers at vendor side.

## <Motivation>

In order to reduce damages by malspam in Japan

## <Activity Overview>

The organization that receives the malspam quickly share information, analyzes it together, and publicly sends out information necessary for countermeasures.

<Ref>50 unknown well-meaning people who protect Japan from scattered emails

<https://xtech.nikkei.com/atcl/nxt/column/18/00138/072700596/>

## <Speakers>

[@bomccss](#)

[@sugimu\\_sec](#)



## 1.2. Observation of Emotet

### <Long-term observation of Emotet attacks>

- Sharing received email templates
  - Emails received mainly by own organization
- Analyze attack
  - Early alert
- Share information with foreign researchers

## 1.3. Today's topic : Emotet

Based on the observed data, we will talk about an analysis of attack campaigns aimed at infecting **Emotet** that have caused serious damage in Japan since the second half of 2019.

- Overview of infection
- Impact in Japan
- Purpose of attack

## 2. What is Emotet?



Office 365

You are attempting to open a file that was created in an earlier version of Microsoft Office.

If the file opens in Protected View, click **Enable Edition** and then click **Enable Content**.

## 2. What is Emotet?

### <Features>

- Compromise by opening malicious documents
- Modular malware
  - Stealing credentials
  - Spread over the network
  - Spread infected emails
  - Transfer of C2 communication
- Infection with other malware via Emotet

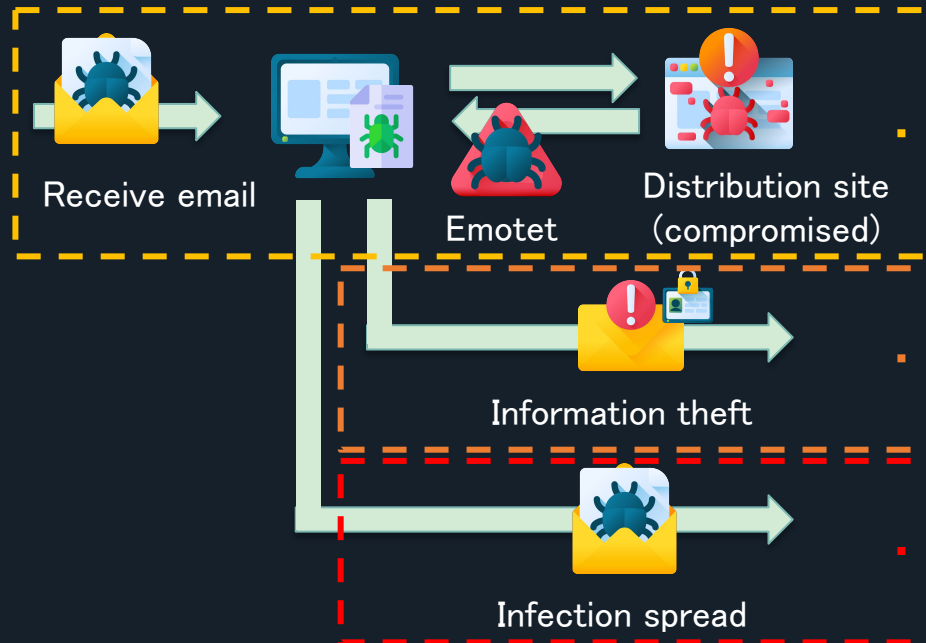
### <When>

Since Japan was added to the attack list in September 2019, malicious emails have been delivered.



## 2.1 Flow of attacks that infect Emotet

- Compromised when opening an email attached document.
- Information is stolen and further spread activities



**1. Receive an email and compromise**

**2. Steal information**

(This section focuses on the theft of email-related information)

**3. Infection spread activity**

(This section focuses on spreading activities by email)

## 2.2.1. Emails targeting Emotet infection

- Sent under the guise of a business partner or related organization
- The contents of stolen emails may be abused
- Document files, password-protected zip files, etc. are attached
- Emails delivered in Japan are mainly based on Japanese

請求書送付のお願い 60479893 2020\_08\_12



宛先



請求書送付のお願い 60479893-2020\_08\_12.doc  
228 KB

お世話になっております。

請求書をお送りいたしましたので

どうぞよろしくお願いいたします。

ホールディングス株

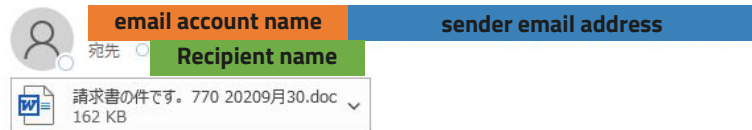
## 2.2.2. Classification of email contents

- Classify email type by following features

	contents of email
Scattered email	<ul style="list-style-type: none"><li>• General-purpose content</li><li>• There is no past reply history in the body and it is sent as a new email</li></ul>
Reply chain type	<ul style="list-style-type: none"><li>• Sent as a reply to the stolen email</li><li>• The history of past emails remains in the body</li></ul>
Fake reply email	<ul style="list-style-type: none"><li>• Many general-purpose contents (a type of scattered mail)</li><li>• At the end of the email body, the content disguised as a past email header starting with "----- Original Message ----" is described.</li></ul>

# (Ref) Scattered email

請求書の件です。770-20209月30



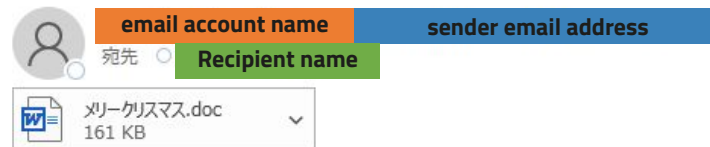
お世話になっております。

一旦、各請求書・清算書をお送り致します。  
どうぞよろしくお願いいたします。

ホールディングス株

E-Mail: **email address**

**personal name**



**personal name** メリークリスマス

いつも大変お世話になっております。

以上、よろしくお願い致します。

-  
**domain name**

# (Ref) Reply email

Fwd: **email subject in history**

 **email account name** **sender email address**  
宛先 **Recipient name**

 契約 #0963038 2009.doc  
159 KB

いつもお世話になっております。

表題の件、DOCにてお送りさせていただきます。

契約書の中身を十分ご確認の上、施主さまへご提示下さいますようお願いいたします。

**personal name**  
**email address**

**email body in history**

RE: **email subject in history**

 **email account name** **sender email address**  
宛先 **Recipient name**

 請求書.zip  
84 KB

いつもお世話になっております。

うお願いします。

対象データ、確認および手続き方法に関しては、添付ファイルを参照ください。  
添付ファイル名: 請求書.zip  
パスワード: L51ylaH


よろしくお願い申し上げます。


**personal name**

**email body in history**

# (Ref) Spoofed reply email

Re: **personal name**

 **email account name** **sender email address**  
**宛先 Recipient name**

 -UH545128.doc  
133 KB

日頃より大変お世話になっております。  
請求書を確認後、3営業日後の返金(着金)となります。


しかしながら、頂きましたご請求書ですが、3点修正が必要です。  
①手数料が反映されておりましたので、請求書に追記ください。(5%)  
②請求書の発行日を記載してください  
③弊社名は「**domain name**」です、ご修正御願います。


宜しくお願いいたします。  
ご不明な点等ございましたらご連絡ください。

**personal name**  
**email address**

-----Original Message-----  
> Date: Thursday, October 14, 2020 20:50  
> From: **Recipient name**  
> To: **email account name**  
> Subject: RE: FW: **email account name**

RE: **personal name**

 **email account name** **sender email address**  
**宛先 Recipient name**

 請求書送付のお願い2020 9月.doc  
160 KB

協力会社各位

お世話になっております。

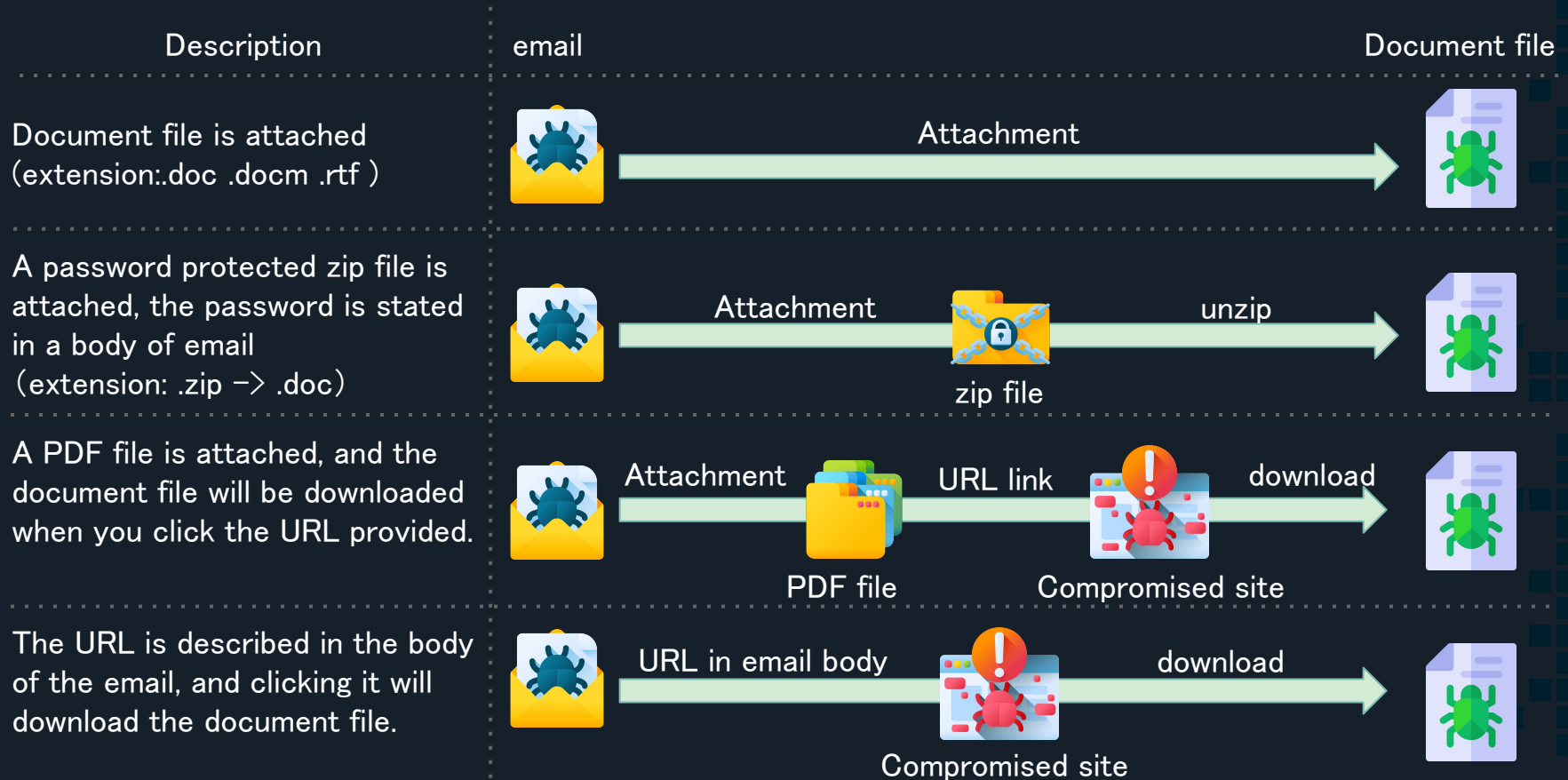
標記の件、2020.09.24に皆様にお送りしたご案内に修正事項がございます。  
以下に要点を記載いたしますのご確認の程お願いいたします。

お心当たりがある業者様は取り急ぎご連絡いただきますようお願いいたします。  
今後の手続きについてご案内いたします。

この度は当方の不手際でご迷惑をお掛けし、大変申し訳ございません。

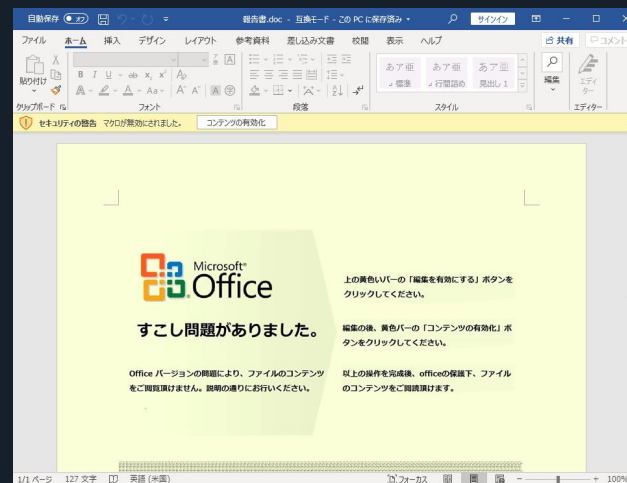
-----Original Message-----  
>> 差出人: **Recipient name**  
>> 日時: Thursday, 2020年9月24, 15:48  
>> 宛先: **email account name**  
>> 件名: Re: Fwd:

## 2.3. Types of navigation to documents



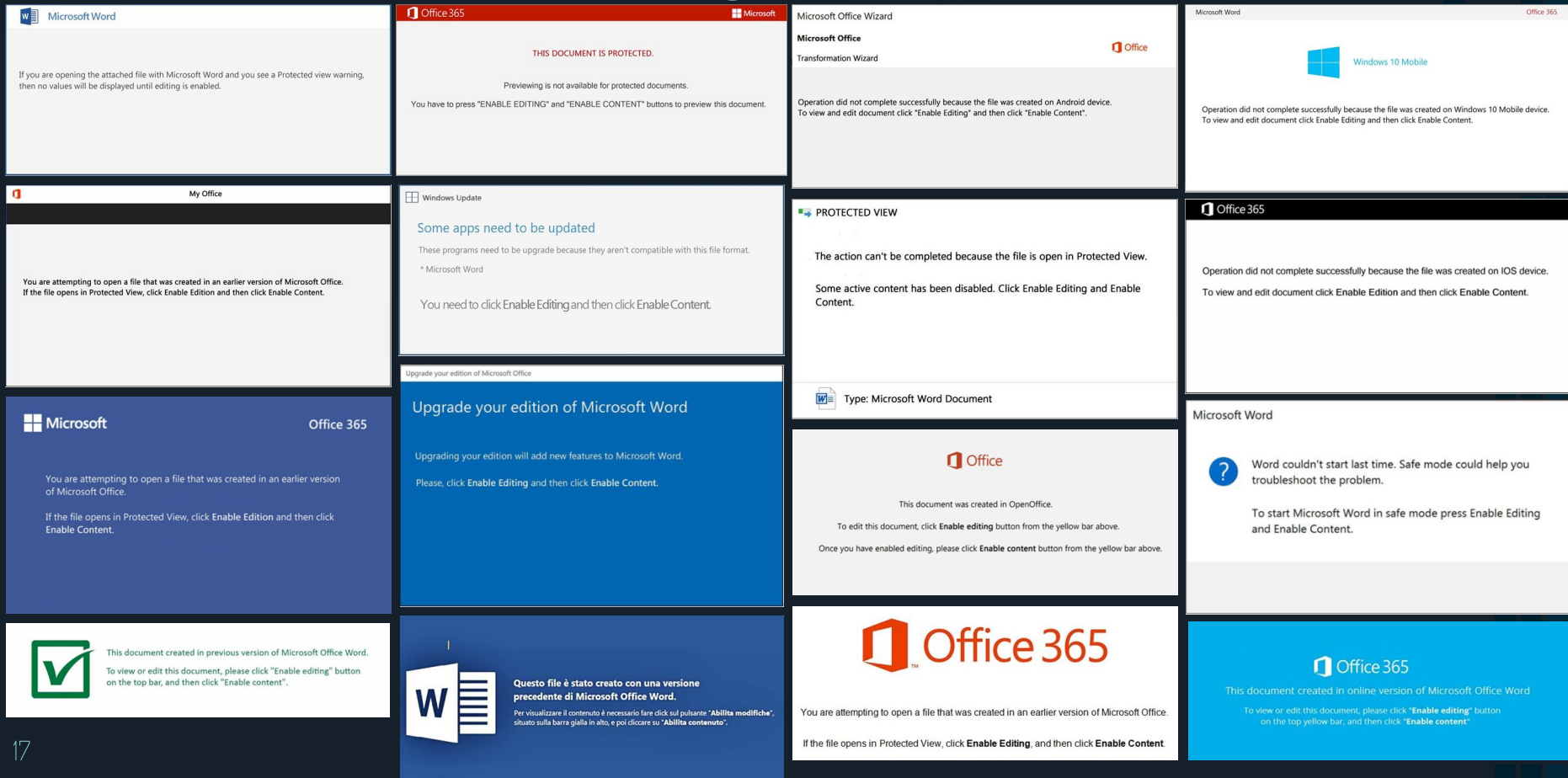
## 2.4. Document file

- Macro works when opening document file and enabling content
- When the script is executed, Emotet is downloaded from the communication destination and executed.
- There is also a document file designed using Japanese
  - Clearly aimed at Japan





# (Ref) Document file design (Partial introduction)



## 2.4.1. Script executed from document file

- PowerShell script or JavaScript
- Multiple URLs are stored in the executed script
  - Compromised site where Emotet is distributed (5~7URL)
  - Emotet downloads and runs when even one is active

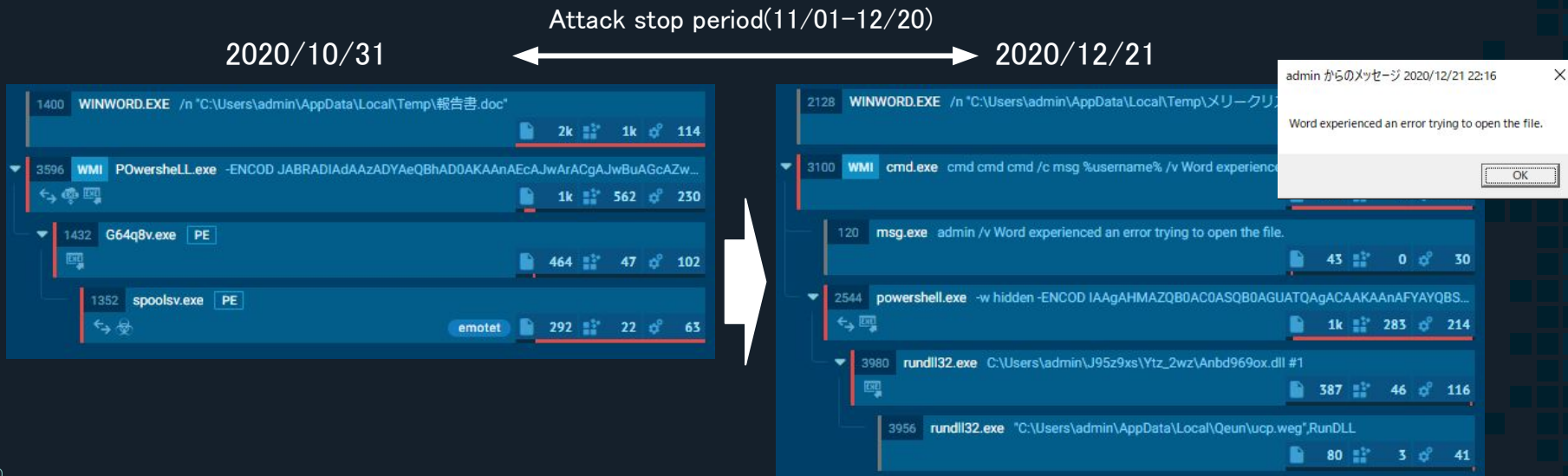
[illegible]

http://n/dooxi-fuel-hf09b/Logs/  
http://aA7YWWX/  
http://n/wp-admin/en-US/  
http://com/streamlabs-obs-rarso/SIGNUP/  
http://0QnnWbk/  
http://m/n/WUGoZ/  
http://ys/

## 2.4.2. Change the flow to infection

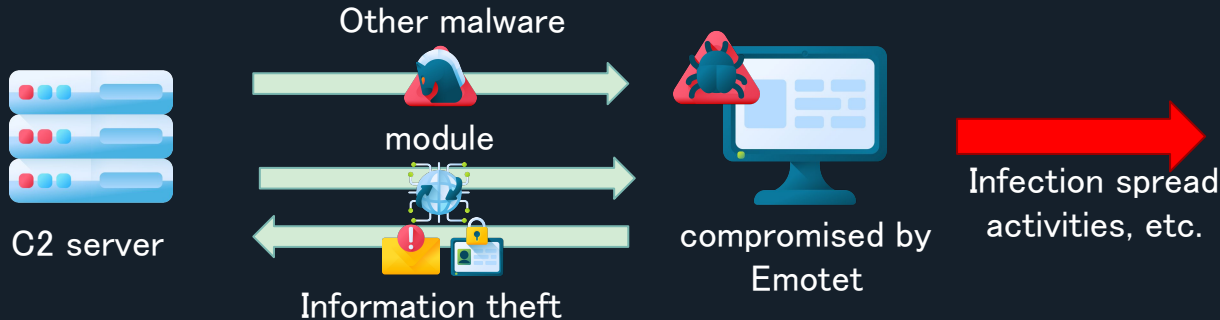
### <update>

- Fake error messages show up
- Run DLL-formatted Emotet with rundll32.exe



## 2.5. Movement after Emotet infection

- Infected with other malware
  - It depends on the time and environment
- Receive the module according to the purpose from the C2 server
  - Example) Information stealer, spoofing email transmission, forwarding of C2 traffice



## 2.5.1. Emotet module

- Emotet is modular malware
  - Information stealer module
    - Email information and browser information
  - Spam module
    - Scattered module and reply module
  - Network spreading module
  - UPnP module
- Downloaded from C2 server according to purpose
- No fraudulent money transfer modules have been identified since 2017



## 2.5.3. Stolen email-related information

- The extracted information is temporarily output to a file
  - The file is deleted once the information is sent to the C2 server

Extracted email address

```
26A.tmp
ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00000000
00000010
00000020 6D 61 69 6C 2E 63 6F 6D 3E 3B 40 68 6F 74 @hot
00000030 mail.com>;
00000040
00000050
00000060
00000070
00000080
00000090 40 67 6D 61 69 6C 2E 63 6F @gmail.co
000000A0 6D 3E 3B m>;
000000B0 40 67 6D 61 69 @gmai
000000C0 6C 2E 63 6F 6D 3E l.com>
```


Extracted received email

```
F4BC.tmp
ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00000000
00000010 Sender name and email address
00000020 40 67 6D 61 69 6C 2E 63 6F 6D 3E 3B @gmail.com>;
00000030
00000040 Recipient name and email address
00000050 6F 74 6D 61 69 6C 2E 63 6F 6D 3E 3B otmail.com>;
00000060 5B 32 30 32 30 [2020
00000070 subject
00000080
00000090
000000A0
000000B0 body
000000C0
:
00000560
00000570 61 70 70 6C 69 63 61 74 69 6F 6E 2F 70 application/p
00000580 64 66 08 00 00 00 31 32 7E 31 2E 70 64 66 64 E8 df....12~1.pdfd.
00000590 00 00 25 50 44 46 2D 31 2E 37 0D 0A 25 B5 B5 B5 ..%PDF-1.7...亀亀
000005A0 B5 0D 0A 31 20 30 20 6F 62 2F 54 ..1 0 obj..<</T
000005B0 79 70 65 2F 43 61 74 61 6C Attachment 67 65
000005C0 73 20 32 20 30 20 52 2F 4C 61 6E 67 28 6A 61 2D
000005D0 4A 50 29 20 2F 53 74 72 75 63 74 54 72 65 65 52 s 2 0 R/Lang(ja-
000005E0 6F 6F 74 20 31 35 20 30 20 52 2F 4D 61 72 6B 49 JP) /StructTreeR
oot 15 0 R/MarkI
```



# (Ref) Stealing email-related information

## Process flow

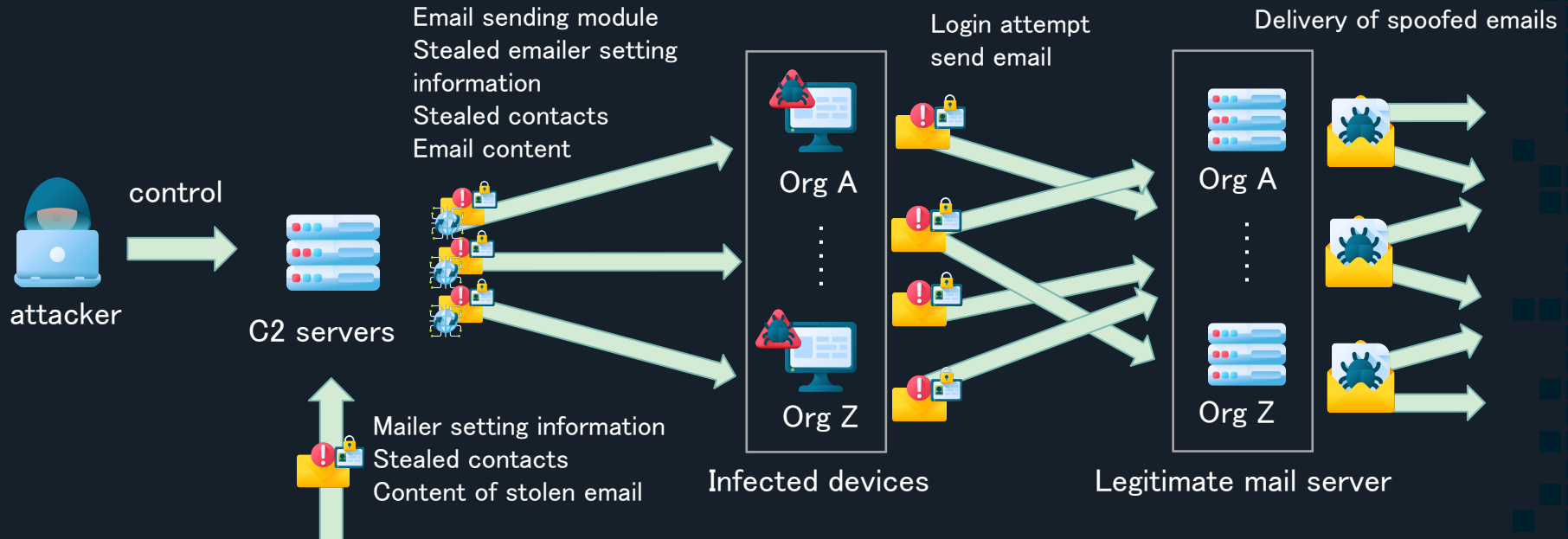


20:08:38.5068946	rundll32.exe	5924	CreateFile	C:\Windows\System32\certutil.exe
20:08:38.5083954	rundll32.exe	5924	QueryStandardInformationFile	C:\Windows\System32\certutil.exe
20:08:38.5087418	rundll32.exe	5924	ReadFile	C:\Windows\System32\certutil.exe
20:08:38.5088474	rundll32.exe	5924	ReadFile	C:\Windows\System32\certutil.exe
20:08:38.5155571	rundll32.exe	5924	CloseFile	C:\Windows\System32\certutil.exe
20:08:38.5159394	rundll32.exe	5924	CreateFile	C:\Users%\AppData\Local\Temp\bo.exe
20:08:38.5164030	rundll32.exe	5924	WriteFile	C:\Users%\AppData\Local\Temp\bo.exe
:				
:				
:				
20:08:38.5272538	bo.exe	5140	CreateFile	C:\Windows\Prefetch\BO_EXE-B000AD3.pf
20:08:38.5278827	bo.exe	5140	CreateFile	C:\Windows\System32
20:08:38.5287116	bo.exe	5140	QueryNameInformationFile	C:\Windows\System32\KernelBase.dll
20:08:38.5287966	bo.exe	5140	QueryNameInformationFile	C:\Windows\System32\KernelBase.dll
20:08:38.5288791	bo.exe	5140	QueryNameInformationFile	C:\Windows\System32\kernel32.dll
:				
:				
:				
20:08:40.4024037	bo.exe	5140	ReadFile	C:\Users%\AppData\Local\Microsoft\Outlook%\com.st
20:08:40.4030548	bo.exe	5140	ReadFile	C:\Users%\AppData\Local\Microsoft\Outlook%\com.st
20:08:40.4033723	bo.exe	5140	ReadFile	C:\Users%\AppData\Local\Microsoft\Outlook%\com.st
20:08:40.4036188	bo.exe	5140	ReadFile	C:\Users%\AppData\Local\Microsoft\Outlook%\com.st
20:08:40.4037045	bo.exe	5140	ReadFile	C:\Users%\AppData\Local\Microsoft\Outlook%\com.st
20:08:40.4046305	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4047106	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4061827	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4062442	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4062957	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4063381	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4064016	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4064218	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4065087	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4065176	bo.exe	5140	WriteFile	C:\Users%\AppData\Local\Temp\F4BC.tmp
20:08:40.4066021	bo.exe	5140	CloseFile	C:\Users%\AppData\Local\Temp\F4BC.tmp



## 2.6. Flow of sending spoofed emails

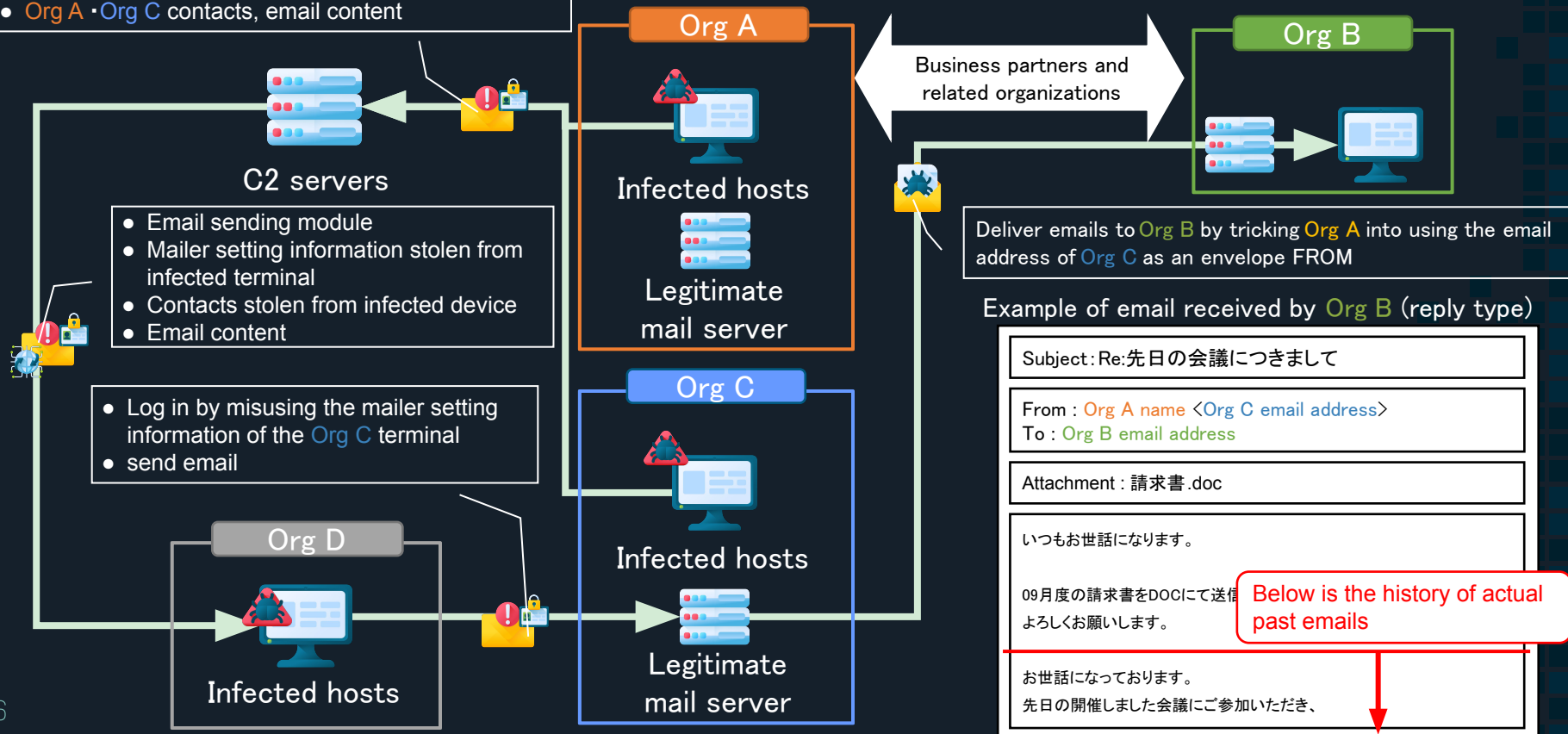
- Spoofed login with stolen email account information
- Deliver emails aimed at infection via a legitimate mail server



## 2.6.1. Image of sending / receiving spoofed emails

- Org A • Org C mailer setting information
- Org A • Org C contacts, email content

\* This is an example of how a reply-type email is sent / received.



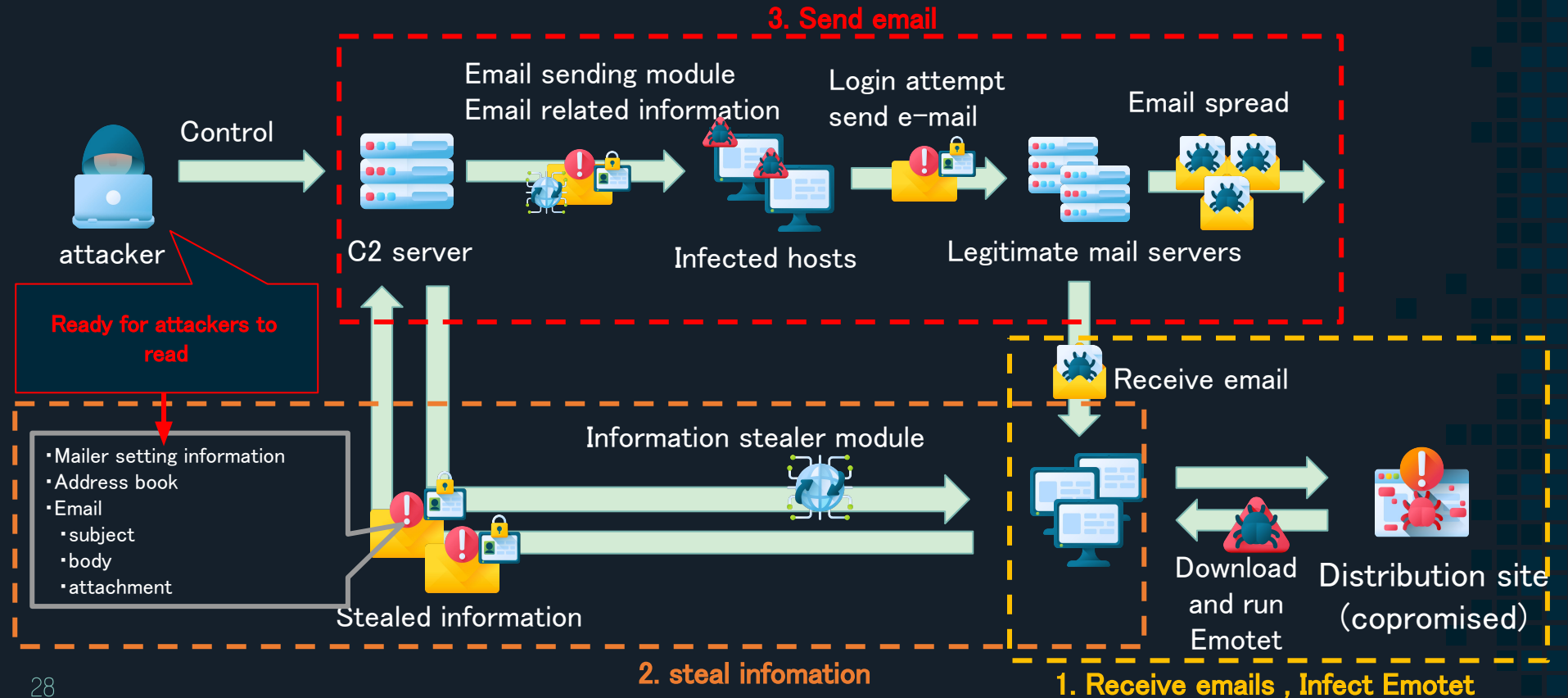
# (Ref) Login enforced from infected hosts

- The stolen email account credentials are misused

## Attempt to log in from infected hosts

時間:14 分前 おおよその場所: ジンバブエ 種類: 通常とは異なるアクティビティが検出されました	このアクティビティが行われてから、アカウントをセキュリティで保護しました。 アカウントを保護するための方法を確認する。
時間:22 分前 おおよその場所: パキスタン 種類: 通常とは異なるアクティビティが検出されました	このアクティビティが行われてから、アカウントをセキュリティで保護しました。 アカウントを保護するための方法を確認する。
時間:24 分前 おおよその場所: タイ 種類: 通常とは異なるアクティビティが検出されました	このアクティビティが行われてから、アカウントをセキュリティで保護しました。 アカウントを保護するための方法を確認する。
時間:29 分前 おおよその場所: 南アフリカ 種類: 通常とは異なるアクティビティが検出されました	このアクティビティが行われてから、アカウントをセキュリティで保護しました。 アカウントを保護するための方法を確認する。

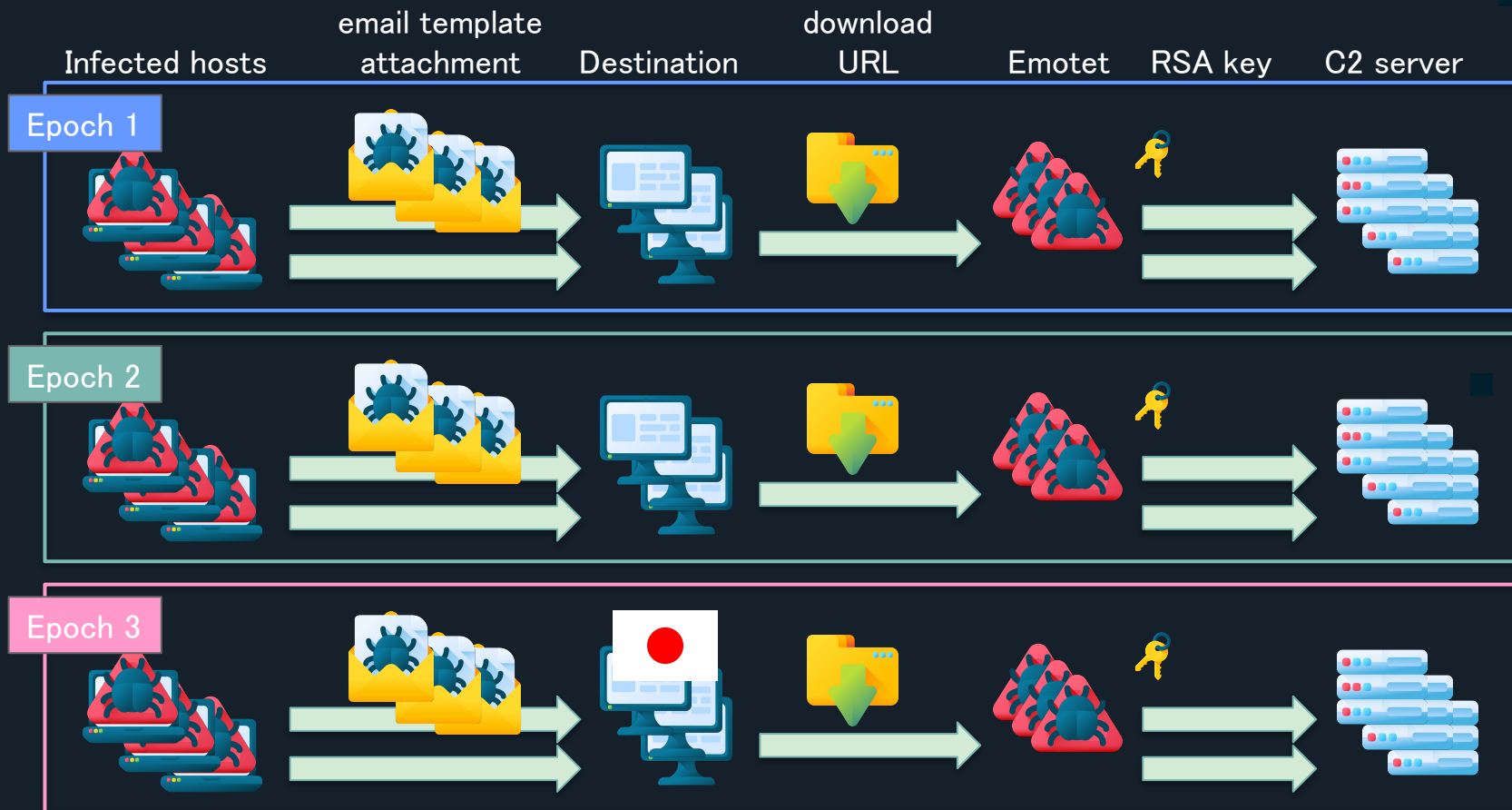
## 2.7. Emotet infection spread cycle by email



## 2.8. Botnet - Epoch

- There are three botnets
  - They are called Epoch1, Epoch2, and Epoch3.
- Unique information for each Epoch
  - Email templates, email address
  - URL of Emotet distribution sites
  - C2 lists and RSA keys included in Emotet
- The main targets are different
  - Japan is a major target for Epoch3 (E3)

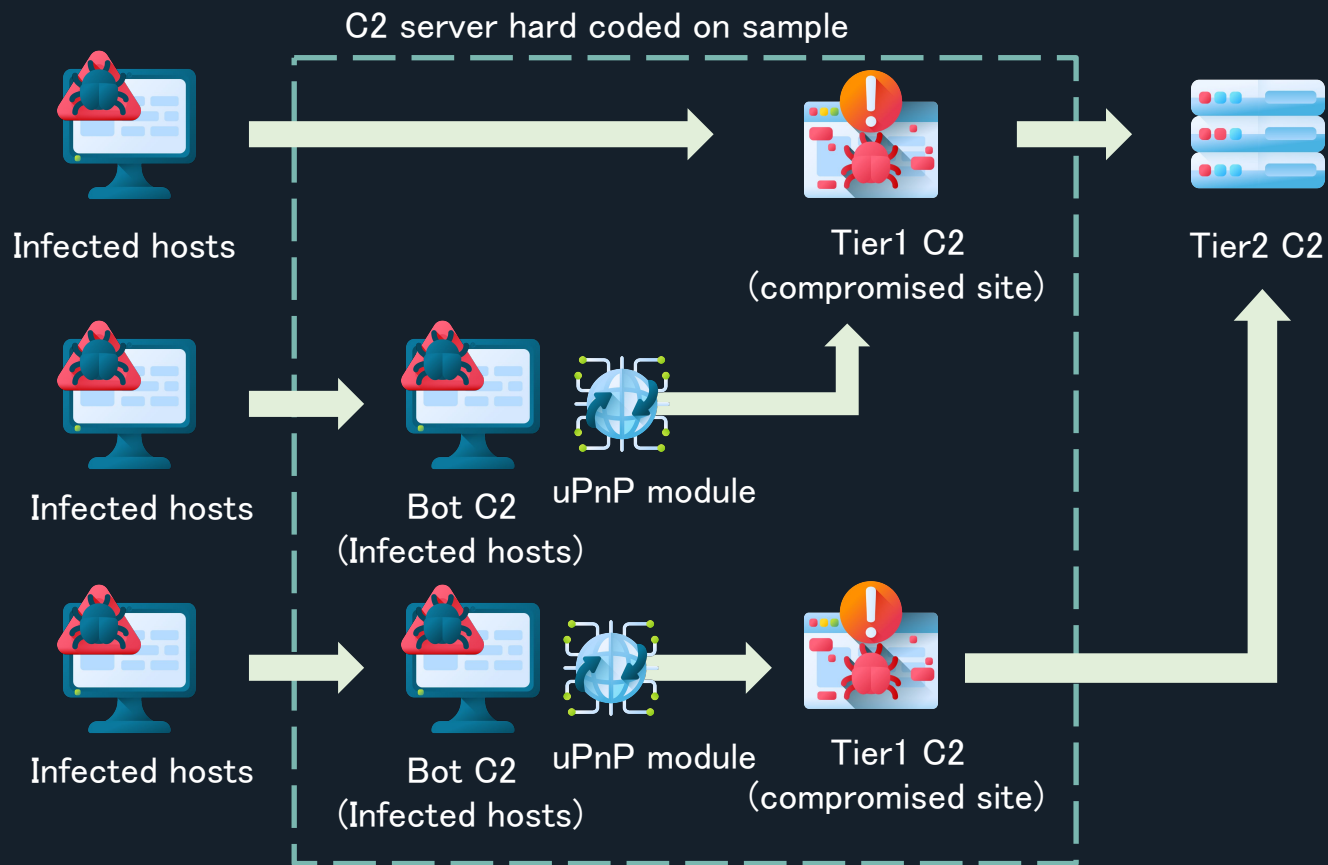
## 2.8.1. Botnet - Epoch



## 2.8.2. C2 server redundancy

- C2 server destination is stored in Emotet
- Each Epoch has a maximum of 128 C2s
- About 80% of C2 servers are Bot C2, therest is Tier 1 C2
  - The BotC2 is an infected host with the UPnP module loaded.
    - Forward communication to Tier1 C2
  - Tier 1 C2 is a compromised Linux server
- And there is a Tier 2 C2 server
  - Tier1 C2 forwards communication to Tier2 C2
- The main purpose is to prevent takedown
- Other modules store the list of other C2 IP addresses

## 2.8.3. C2 server redundancy

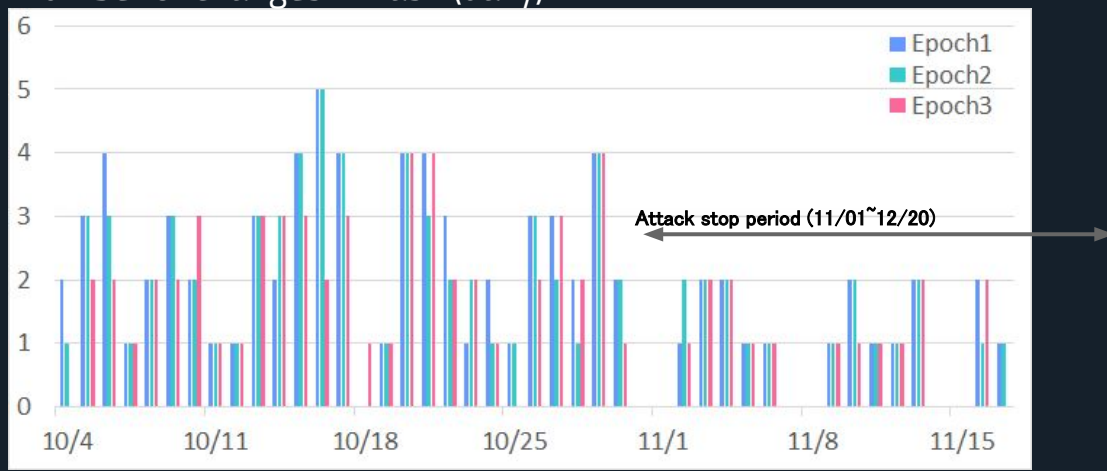




## 2.8.4. Function of evasion detection

- Evasion detection by antivirus software
  - Unique hash for each infected host
  - Periodic update of Emotet (change of hash)
    - Up to 5 times a day
    - In addition to holidays such as Sat. and Sun., the attack stop date is also updated

Number of changes in hash (daily)



### 3. Impact of Emotet on Japan



This document only available for desktop or laptop versions of Microsoft Office Word.

To open the document, follow these steps:

Click Enable editing button from the yellow bar above,  
Once you have enabled editing, please click Enable content button.

## 3.1. Attack on Japan

Time (date)	Activity	Remarks
2019/04/12	Receive emails written in Japanese (Temporary)	Unconfirmed second malware
09/27	Japan is targeted in earnest	Confirmed second malware
Around 2019/11	Increased number of infections due to reply emails	Emails that are not in Japanese
11/23	Attacks on Japan intensify	Email written in Japanese
2020/02/06	Attacks stopped around the world	
07/17	Attacks resume around the world	

## 3.1. Attack on Japan

Time (date)	activity	Remarks
2020/08/28	Japan became a target in all Epochs	Rapid increase in emails to Japan
08/31	Increase in number of infections in Japan	Approximately 200% increase compared to 28 <sup>th</sup>
09/02	Password protected zip files have been attached	Factors behind the rapid increase in infection
09/25	Document files with Japanese design started to be used	
10/31	Attacks stopped around the world	
12/21	Attacks resume around the world	Few to Japan

## 3.2. The days targeted Japan

### Emotet email sending date and Japan targeted date

<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2019/09</td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr><tr><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td></tr><tr><td>29</td><td>30</td><td></td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2019/09							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2019/10</td></tr><tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td></tr><tr><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2019/10									1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2019/11</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>1</td><td>2</td></tr><tr><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr><tr><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td></tr><tr><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td></tr></table>	日	月	火	水	木	金	土	2019/11												1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2019/12</td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr><tr><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td></tr><tr><td>29</td><td>30</td><td>31</td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2019/12							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																		
日	月	火	水	木	金	土																																																																																																																																																																																																															
2019/09																																																																																																																																																																																																																					
1	2	3	4	5	6	7																																																																																																																																																																																																															
8	9	10	11	12	13	14																																																																																																																																																																																																															
15	16	17	18	19	20	21																																																																																																																																																																																																															
22	23	24	25	26	27	28																																																																																																																																																																																																															
29	30																																																																																																																																																																																																																				
日	月	火	水	木	金	土																																																																																																																																																																																																															
2019/10																																																																																																																																																																																																																					
		1	2	3	4	5																																																																																																																																																																																																															
6	7	8	9	10	11	12																																																																																																																																																																																																															
13	14	15	16	17	18	19																																																																																																																																																																																																															
20	21	22	23	24	25	26																																																																																																																																																																																																															
27	28	29	30	31																																																																																																																																																																																																																	
日	月	火	水	木	金	土																																																																																																																																																																																																															
2019/11																																																																																																																																																																																																																					
					1	2																																																																																																																																																																																																															
3	4	5	6	7	8	9																																																																																																																																																																																																															
10	11	12	13	14	15	16																																																																																																																																																																																																															
17	18	19	20	21	22	23																																																																																																																																																																																																															
24	25	26	27	28	29	30																																																																																																																																																																																																															
日	月	火	水	木	金	土																																																																																																																																																																																																															
2019/12																																																																																																																																																																																																																					
1	2	3	4	5	6	7																																																																																																																																																																																																															
8	9	10	11	12	13	14																																																																																																																																																																																																															
15	16	17	18	19	20	21																																																																																																																																																																																																															
22	23	24	25	26	27	28																																																																																																																																																																																																															
29	30	31																																																																																																																																																																																																																			
<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/01</td></tr><tr><td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td></tr><tr><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr><tr><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td></tr></table>	日	月	火	水	木	金	土	2020/01										1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/02</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr><tr><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr><tr><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td></tr><tr><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr></table>	日	月	火	水	木	金	土	2020/02													1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/03</td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr><tr><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td></tr><tr><td>29</td><td>30</td><td>31</td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/03							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/04</td></tr><tr><td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td></tr><tr><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr><tr><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/04										1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30																
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/01																																																																																																																																																																																																																					
			1	2	3	4																																																																																																																																																																																																															
5	6	7	8	9	10	11																																																																																																																																																																																																															
12	13	14	15	16	17	18																																																																																																																																																																																																															
19	20	21	22	23	24	25																																																																																																																																																																																																															
26	27	28	29	30	31																																																																																																																																																																																																																
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/02																																																																																																																																																																																																																					
						1																																																																																																																																																																																																															
2	3	4	5	6	7	8																																																																																																																																																																																																															
9	10	11	12	13	14	15																																																																																																																																																																																																															
16	17	18	19	20	21	22																																																																																																																																																																																																															
23	24	25	26	27	28	29																																																																																																																																																																																																															
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/03																																																																																																																																																																																																																					
1	2	3	4	5	6	7																																																																																																																																																																																																															
8	9	10	11	12	13	14																																																																																																																																																																																																															
15	16	17	18	19	20	21																																																																																																																																																																																																															
22	23	24	25	26	27	28																																																																																																																																																																																																															
29	30	31																																																																																																																																																																																																																			
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/04																																																																																																																																																																																																																					
			1	2	3	4																																																																																																																																																																																																															
5	6	7	8	9	10	11																																																																																																																																																																																																															
12	13	14	15	16	17	18																																																																																																																																																																																																															
19	20	21	22	23	24	25																																																																																																																																																																																																															
26	27	28	29	30																																																																																																																																																																																																																	
<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/05</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td>1</td><td>2</td></tr><tr><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr><tr><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td></tr><tr><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td></tr><tr><td>31</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/05												1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31							<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/06</td></tr><tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr><tr><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td></tr><tr><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td></tr><tr><td>28</td><td>29</td><td>30</td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/06								1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30					<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/07</td></tr><tr><td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td></tr><tr><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr><tr><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td></tr></table>	日	月	火	水	木	金	土	2020/07										1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/08</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr><tr><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr><tr><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td></tr><tr><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr><tr><td>30</td><td>31</td><td></td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/08													1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/05																																																																																																																																																																																																																					
					1	2																																																																																																																																																																																																															
3	4	5	6	7	8	9																																																																																																																																																																																																															
10	11	12	13	14	15	16																																																																																																																																																																																																															
17	18	19	20	21	22	23																																																																																																																																																																																																															
24	25	26	27	28	29	30																																																																																																																																																																																																															
31																																																																																																																																																																																																																					
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/06																																																																																																																																																																																																																					
	1	2	3	4	5	6																																																																																																																																																																																																															
7	8	9	10	11	12	13																																																																																																																																																																																																															
14	15	16	17	18	19	20																																																																																																																																																																																																															
21	22	23	24	25	26	27																																																																																																																																																																																																															
28	29	30																																																																																																																																																																																																																			
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/07																																																																																																																																																																																																																					
			1	2	3	4																																																																																																																																																																																																															
5	6	7	8	9	10	11																																																																																																																																																																																																															
12	13	14	15	16	17	18																																																																																																																																																																																																															
19	20	21	22	23	24	25																																																																																																																																																																																																															
26	27	28	29	30	31																																																																																																																																																																																																																
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/08																																																																																																																																																																																																																					
						1																																																																																																																																																																																																															
2	3	4	5	6	7	8																																																																																																																																																																																																															
9	10	11	12	13	14	15																																																																																																																																																																																																															
16	17	18	19	20	21	22																																																																																																																																																																																																															
23	24	25	26	27	28	29																																																																																																																																																																																																															
30	31																																																																																																																																																																																																																				
<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/09</td></tr><tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td></tr><tr><td>27</td><td>28</td><td>29</td><td>30</td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/09									1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/10</td></tr><tr><td></td><td></td><td></td><td></td><td>1</td><td>2</td><td>3</td></tr><tr><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td></tr><tr><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td></tr><tr><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr></table>	日	月	火	水	木	金	土	2020/10											1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/11</td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr><tr><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td></tr><tr><td>29</td><td>30</td><td></td><td></td><td></td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/11							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						<table><tr><th>日</th><th>月</th><th>火</th><th>水</th><th>木</th><th>金</th><th>土</th></tr><tr><td colspan="7">2020/12</td></tr><tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td></tr><tr><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td><td></td></tr></table>	日	月	火	水	木	金	土	2020/12									1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/09																																																																																																																																																																																																																					
		1	2	3	4	5																																																																																																																																																																																																															
6	7	8	9	10	11	12																																																																																																																																																																																																															
13	14	15	16	17	18	19																																																																																																																																																																																																															
20	21	22	23	24	25	26																																																																																																																																																																																																															
27	28	29	30																																																																																																																																																																																																																		
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/10																																																																																																																																																																																																																					
				1	2	3																																																																																																																																																																																																															
4	5	6	7	8	9	10																																																																																																																																																																																																															
11	12	13	14	15	16	17																																																																																																																																																																																																															
18	19	20	21	22	23	24																																																																																																																																																																																																															
25	26	27	28	29	30	31																																																																																																																																																																																																															
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/11																																																																																																																																																																																																																					
1	2	3	4	5	6	7																																																																																																																																																																																																															
8	9	10	11	12	13	14																																																																																																																																																																																																															
15	16	17	18	19	20	21																																																																																																																																																																																																															
22	23	24	25	26	27	28																																																																																																																																																																																																															
29	30																																																																																																																																																																																																																				
日	月	火	水	木	金	土																																																																																																																																																																																																															
2020/12																																																																																																																																																																																																																					
		1	2	3	4	5																																																																																																																																																																																																															
6	7	8	9	10	11	12																																																																																																																																																																																																															
13	14	15	16	17	18	19																																																																																																																																																																																																															
20	21	22	23	24	25	26																																																																																																																																																																																																															
27	28	29	30	31																																																																																																																																																																																																																	

**Yellow :**

Emotet emails are sent,  
not for Japan

**Red :**

Emotet emails are sent,  
targeting Japan

Japan is included in the  
target in about half

### 3.3. Changes in email trends and characteristics

- Early attack
  - Machine translation from general English content
  - Contents and attachments disguised as documents and invoices
- Themes that match the time will be used (from 2019/12)
  - Bonus, Christmas, COVID-19
- Fluent Japanese text is used (from 2020/01)
  - Diversion from stolen emails and learning on the attacker side
- Reply type is used consistently
  - Templates are getting more and more complicated

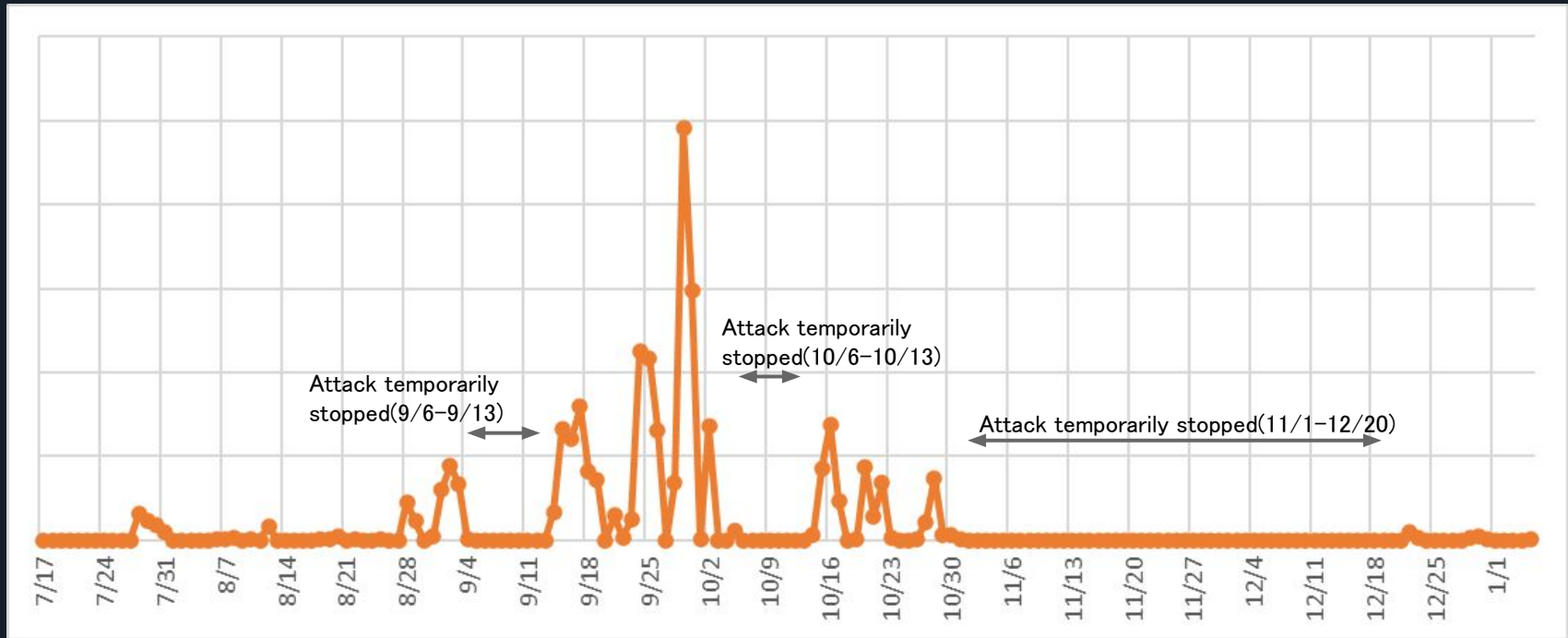
# (Ref) Typical email templates and frequencies

types	First seen	Last seen	counts	subject (esample)	attachment (example)	remarks
invoice	2019/4/12	2020/8/13	8	請求書の送信	47434999183 703679.doc	
General	2019/9/27	2020/10/17	37	ドキュメント	PO# 08182020Ex.doc	
invoice	2019/11/27	2020/12/30	62	請求書の件です。[数字日付]	請求書の件です。 167204 20200728.doc	
bounus	2019/12/9	2020/12/30	17	賞与支払届	12月賞与 .doc	
Christmas	2019/12/18	2020/12/29	6	メリークリスマス	メリークリスマス .doc	
meeting notice	2020/1/14	2020/2/3	16	会議開催通知	会議開催通知 .doc	
invitation to meeting	2020/1/17	2020/12/30	34	会議への招待 [宛先domain]	ビジネス会議への招待 .doc	
COVID-19	2020/1/28	2020/9/15	7	山城南保健所福祉室 [日付]	通知 [日付].doc	
meeting agenda	2020/8/12	2020/9/30	13	金曜日の次の会議の議題。	金曜日の会議のチェックリスト。	
partner companies	2020/9/1	2020/10/28	25	[宛先表示名]	変化[日付].doc	Also used in reply type
Trendmicro	2020/9/3	2020/9/28	9	トレンドマイクロ・	カスタマー満足度アンケート .doc	
update	2020/9/25	2020/10/28	14	[宛先表示名]	更新のご案内 .doc	Also used in reply type
Additions	2020/9/29	2020/10/20	9	[宛先表示名]	追加分も .doc	Also used in reply type

## 3.4. Scale of emails addressed to Japan (daily)

### Number of emails addressed to jp domain email addresses

(Calculated based on observed email data, 2020/07–2021/01)



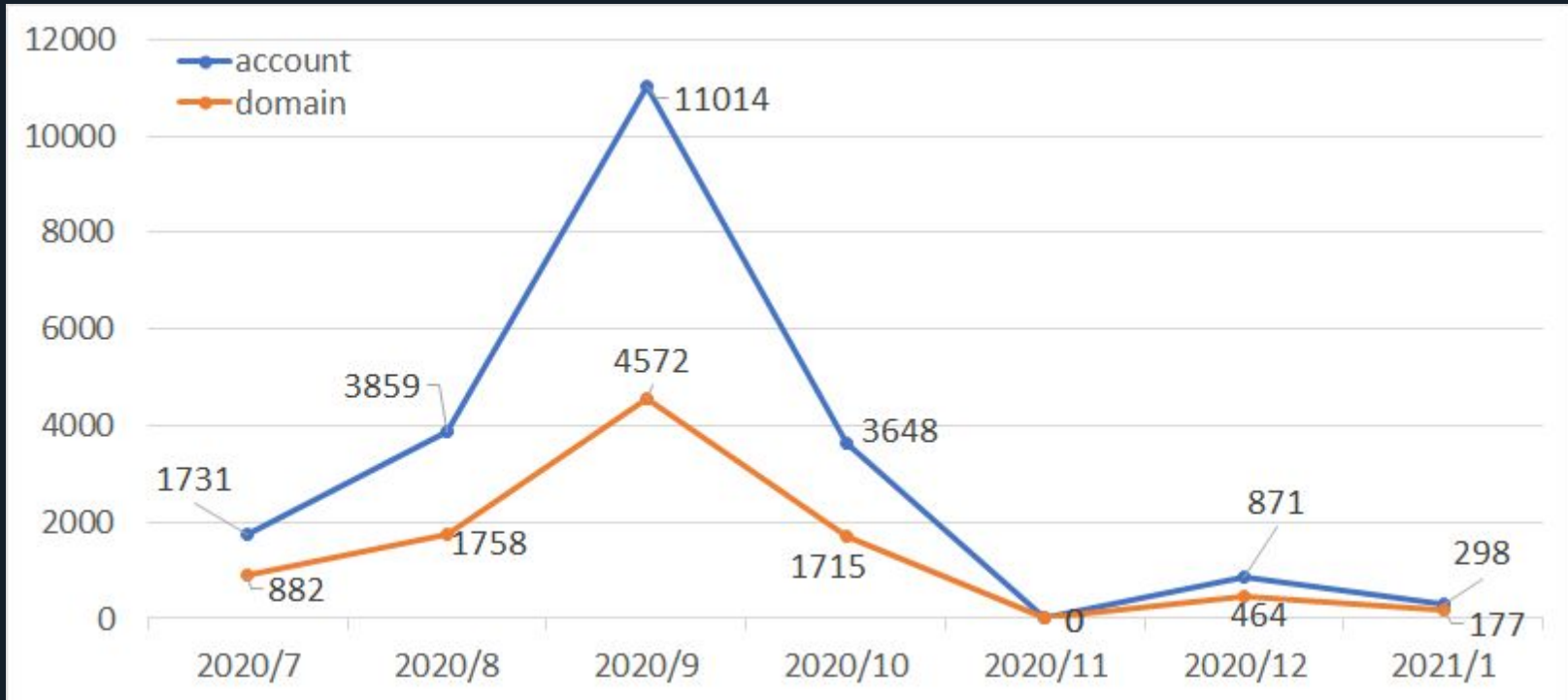
\*The actual number is difficult to show due to various reasons, but it is on the scale of 10,000



## 3.5. Changes in the number of infections (monthly)

### Number of email accounts stolen and abused in .jp domain

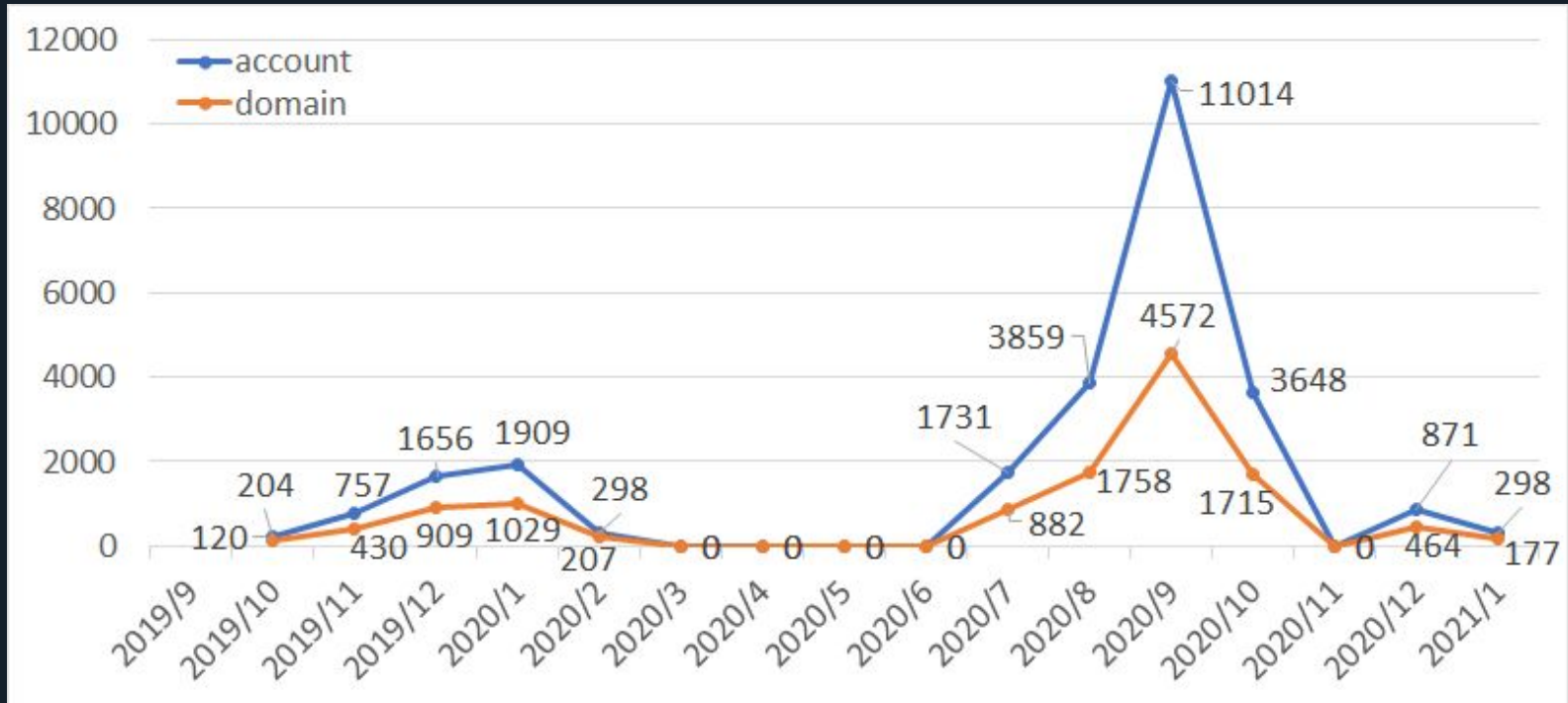
(Calculated based on observed email data, 2020/07–2021/01)



# (Ref) Changes in the number of infections (monthly)

## Number of email accounts stolen and abused in jp domain

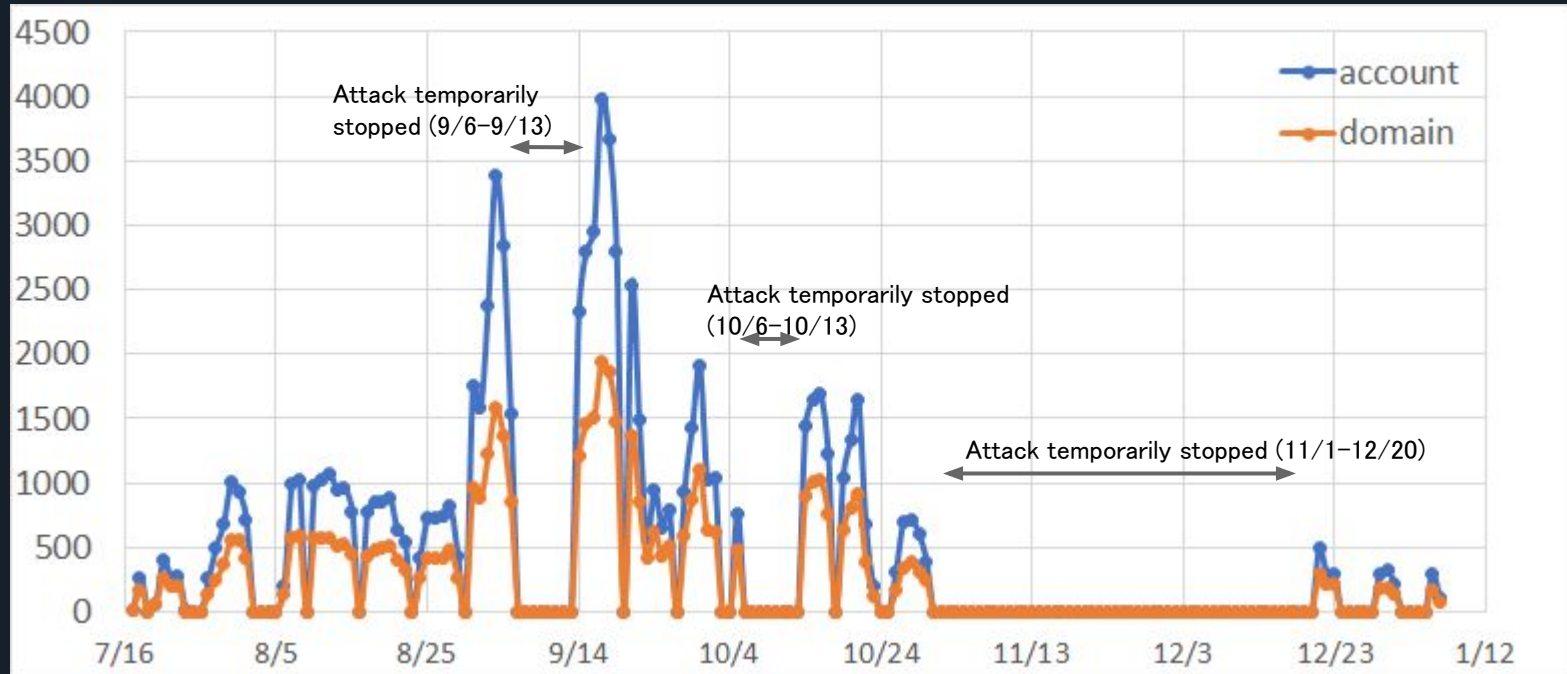
(Calculated based on observed email data 2019/09–2021/01)



## 3.6. Changes in the number of infections (daily)

### Number of email accounts stolen and abused in .jp domain

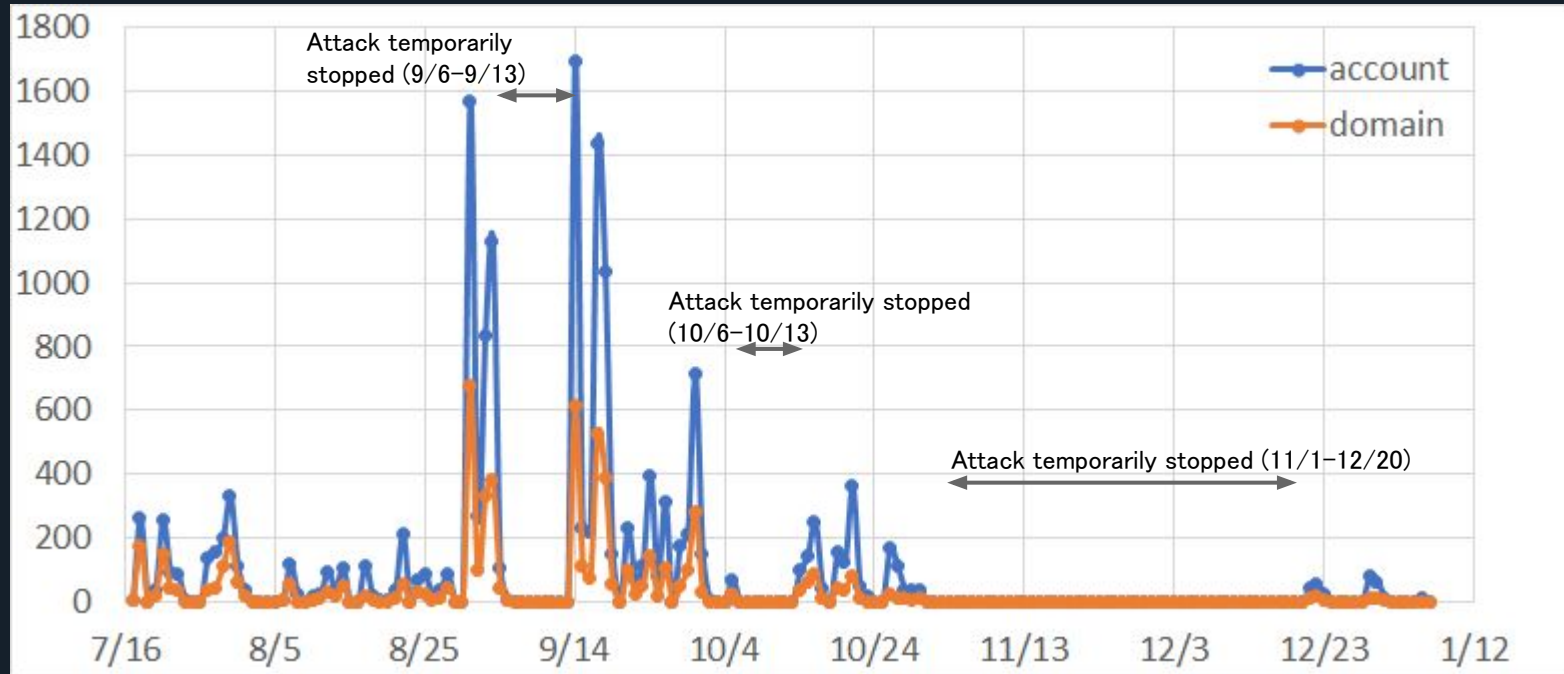
(Calculated based on observed email data, 2020/07–2021/01)



## 3.7. Changes in the number of new infections (daily)

### Number of new email accounts stolen and abused in .jp domain

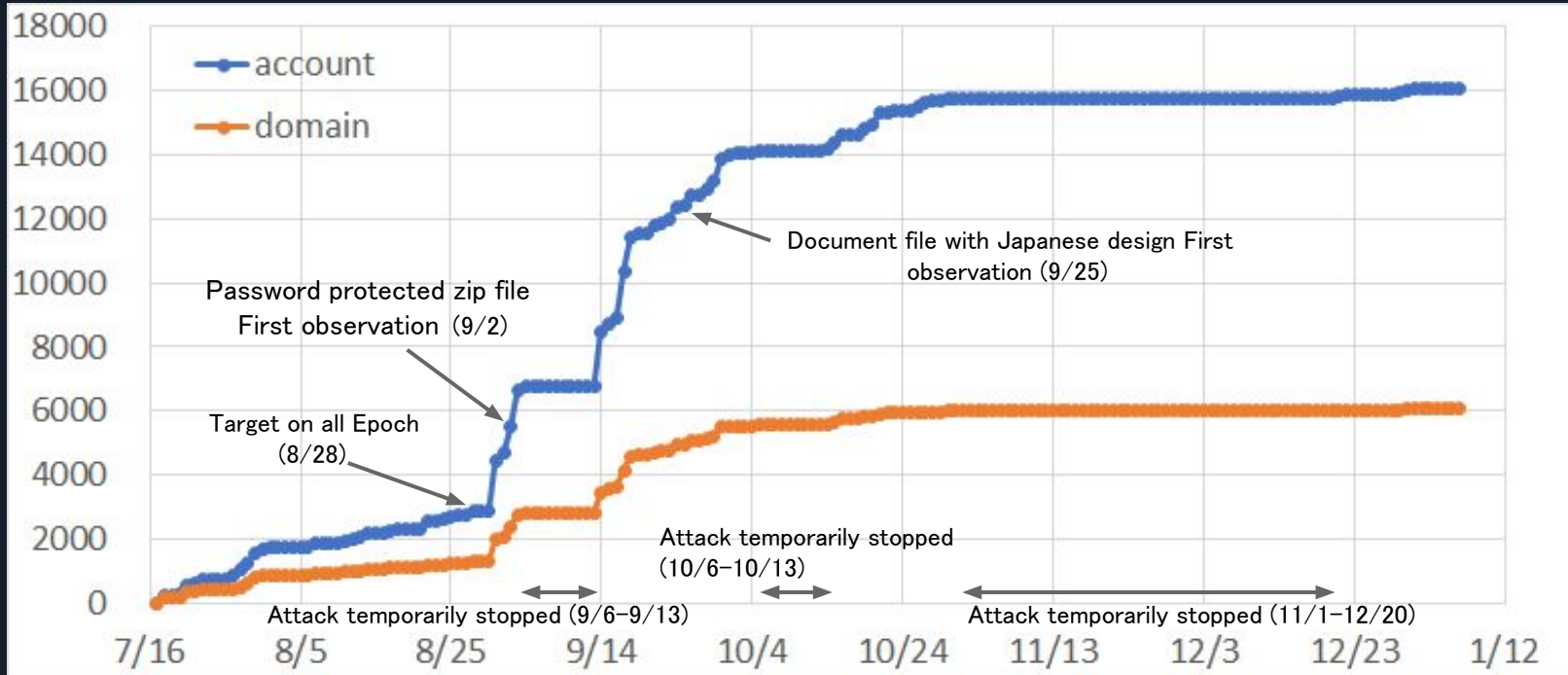
(Calculated based on observed email data, 2020/07–2021/01)



## 3.8. Changes in the cumulative number of infections (daily)

### Cumulative number of email accounts stolen and abused in .jp domain

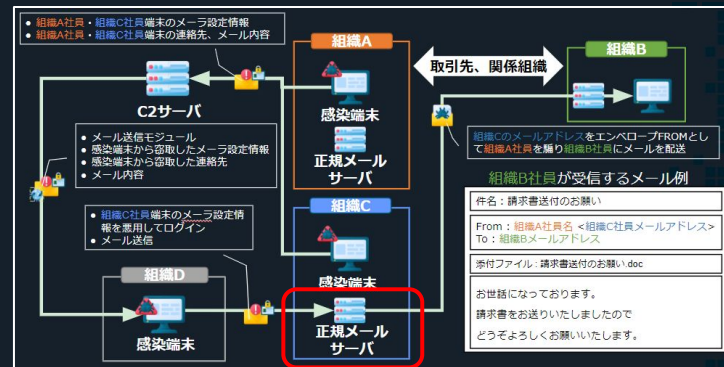
(Calculated based on observed email data, 2020/07–2021/01)



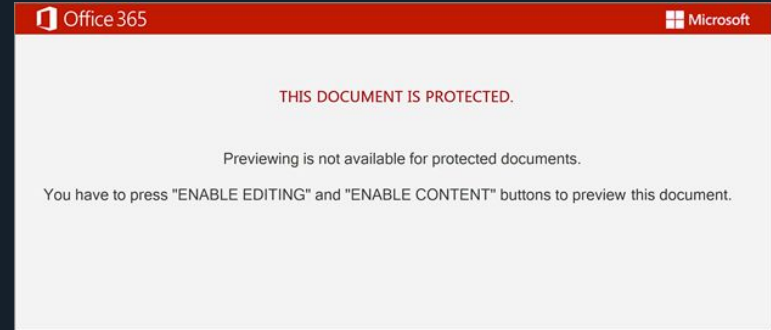
# (Ref) About the number of .jp email accounts

## <Points to remember>

- Only .jp (Japan included in others is not counted for convenience)
- The number was abused by the sender of the email (red frame in the lower right figure), not the exact number of infections.
  - Multiple email accounts may be stolen from one device or none may be stolen
- Affected by the amount of email sent
  - If the amount of transmission is small, the number of observations may decrease and deviate from the tendency.



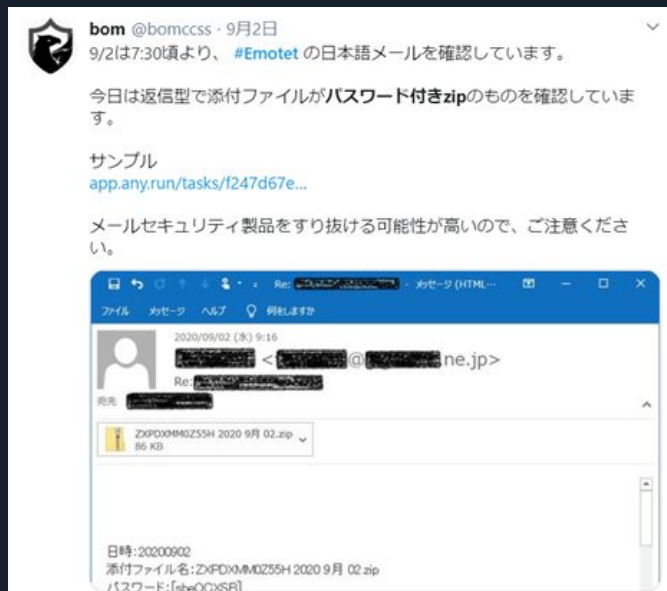
## 4. Damage reduction measures



## 4.1. Information sharing

### Information sharing and alerting the latest Emotet trends on Twitter etc.

#### Observing password protected zip



**bom** @bomccss · 9月2日  
9/2は7:30頃より、[#Emotet](#) の日本語メールを確認しています。

今日は返信型で添付ファイルがパスワード付きzipのものを確認しています。


サンプル  
[app.any.run/tasks/f247d67e...](#)

メールセキュリティ製品をすり抜ける可能性が高いので、ご注意ください。

**添付ファイル**  
Z\FDX\M40255H 2020 9月 02.zip  
86 KB

日時: 20200902  
添付ファイル名: Z\FDX\M40255H 2020 9月 02.zip  
パスワード: [redacted]

#### Response procedures after infection



**bomb\_log**  
id:bomccss

**Emotet感染時の対応**

マルウェア Emotet (エモテット) に感染したら? 感染が疑われる際の対応や感染有無の確認、駆除の方法、について 対応方法を記載しています。

2020-01-27 13:23 ★★★★★ **20 users**

---

**bomb\_log**  
id:bomccss

**マルウェアEmotetの活動再開 (2020/07/17-)**

2019年より日本に向けても活動を行っているマルウェアEmotet (エモテット) (2020/02/07以降活動休止) が2020/07/17より約5ヶ月ぶりに活動を再開しました。 ※ (2020/12/22追記) 2020/10/31の休止...

2020-07-22 06:30 ★★★★★ **11 27 users**



## 4.1. Information sharing

- email template
  - New coronavirus-themed email
  - Emails that trick Trend Micro
- Early detection of new methods
  - Use password protected zip files
- Document file with Japanese design
- Share payload URLs (Register with URLHaus)

## 4.1.1. Heads up

- Alerts are mainly sent out by the community, but our companies may help if necessary.
- 2019/11/27 JPCERT/CC Issued Emotet alert
  - 2019/12/02 Published blog How to Respond to Emotet Infection (FAQ)

<https://blogs.ipcert.or.jp/en/2019/12/emotetfaq.html>

11/28 Chief Cabinet Secretary calls attention to Emotet

2019-11-28 19:17 | 政治

菅官房長官、P Cウイルスで注意喚起＝「エモテット」

[Twitter](#) [Facebook](#) [LINE](#)

菅義偉官房長官は28日の記者会見で、国内で「エモテット」と呼ばれるコンピューターウイルスの感染被害が発生していると明らかにした。菅氏は「行政機関、2020年東京（五輪・パラリンピック）大会に関わる事業者」に注意喚起を行っている。引き続き状況把握に努めるとともに、被害拡大防止のため必要な注意喚起を行っていきたい」と説明した。

エモテットは、実在の組織などになりすましたメールに添付して送り付けられ、感染するとメール本文やパスワードなどが窃取される。その情報を基に新たななりすましメールが送信され、被害が欧米を中心に拡散している。

【時事通信社】



佐藤 研(Ken Sajo)

December 4, 2019

### How to Respond to Emotet Infection (FAQ)

[Tweet](#) [Email](#)

Since October 2019, there has been a growing number of Emotet infection cases in Japan. JPCERT/CC issued a security alert as follows:

Alert Regarding Emotet Malware Infection

<https://www.ipcert.or.jp/english/at/2019/at190044.html>

The purpose of this entry is to provide instructions on how to check if you are infected with Emotet and what you can do in case of infection (based on the information available as of December 2019). If you are not familiar with the detailed investigation methods described here, it is recommended that you consult with security vendors who can assist you.

## 4.2. Global cooperation

- Emotet is a global threat, and there is a global group “[Cryptolaemus](#)” to counter Emotet
  - Gathering security experts from around the world
- Cooperation to share information from Japan
  - Information sharing as TTPs
  - Complement the time zone
- Register the communication destination of Emotet in URLHaus
  - Anyone can block malicious traffic with URLHaus feed



Ref: <https://paste.cryptolaemus.com/>

<https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/>

## 4.3. Report of distribution site

- Early detection of falsified sites
  - Site where document files are distributed
  - Site where Emotet itself is distributed
- Contact the IT service provider Abuse
- Contact the organization's CSIRT or security officer

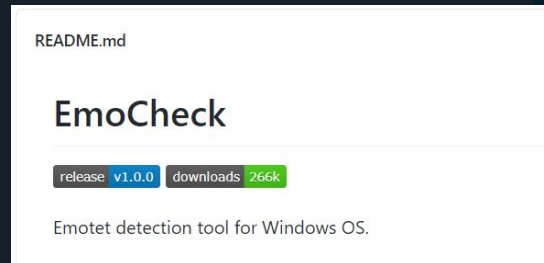
→ Reduce the number of new infections by cutting off the flow of infection

## 4.4. Notification to misused email addresses

- Observe email addresses abused for sending
- Notify abused email addresses
  - Be aware of the infection and have it dealt with
  - More than 4,500 notifications so far
  - Most are personal email addresses such as ISPs
- Cases that have already been noticed and dealt with
- Cases where the remedy is unknown / insufficient even if they know it
  - If necessary, consult with us by email or phone.

## 4.5. EmoCheck

- It may be difficult to explain or respond depending on the other party
    - Need to be able to check for Emotet infection by yourself
  - Emotet has unique traces and naming conventions
    - Based on that, it is possible to check for infection.
    - Propose a concept and request development
      - Released **EmoCheck**
- <https://github.com/JPCERTCC/EmoCheck/releases>



## 5. Emotet Campaign Analysis



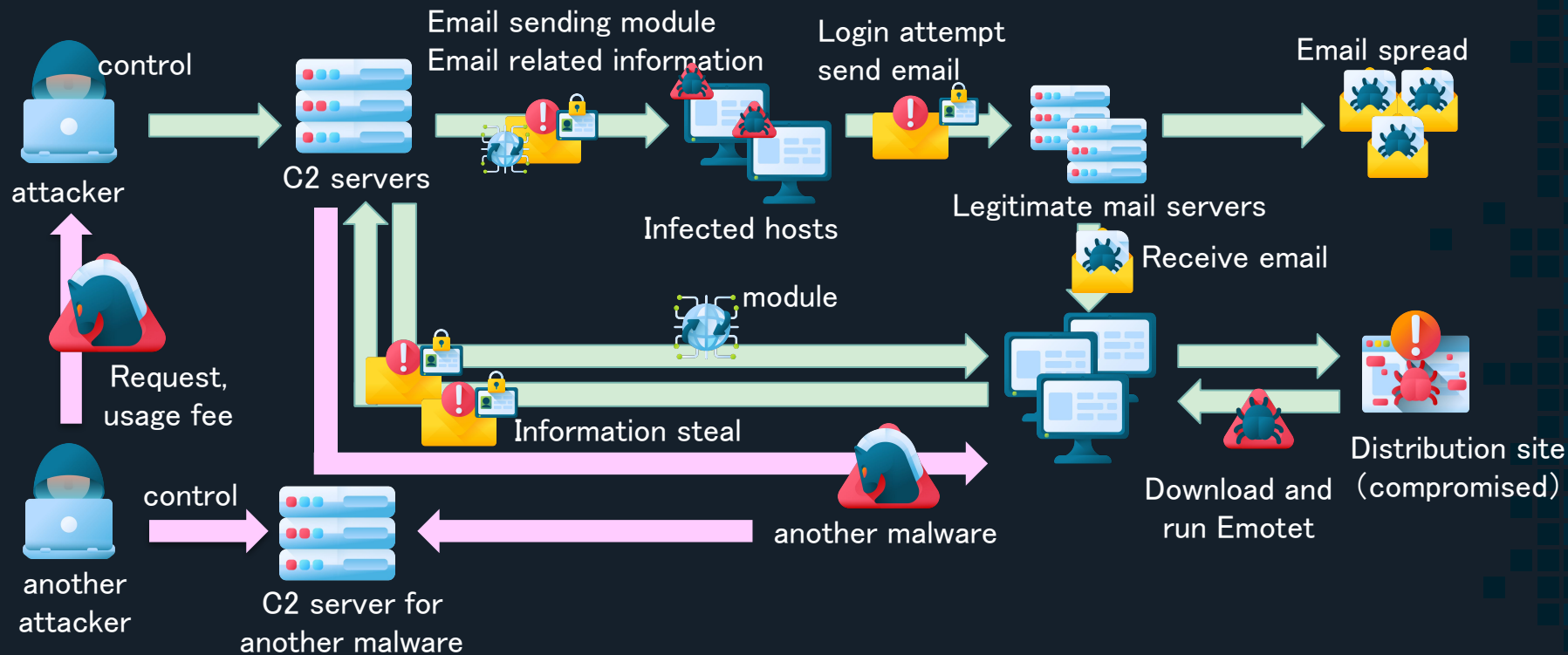
## 5.1. Purpose of Emotet campaign

- **Two groups** are involved in Emotet attacks
  - The side that delivers email using Emotet
    - Attack group operating Emotet
  - The side that uses Emotet to infect other malware
    - Another attack group that wants to use another malware



## 5.1. Purpose of Emotet campaign

- Two groups are involved in Emotet attacks



## 5.2. Attack group that operates Emotet

- Emotet is malware used by a single group
- Attack groups are called Mealybugs, Mummy Spider, TA542, etc. (all the same)
  - Cryptolaemus calls **Ivan**
- Emotet is a tool for infecting other malware
  - They are getting **royalties** from another attack group by infecting another malware

## 5.2. Purpose of the attack group that operates Emotet

By increasing the number of infected hosts of Emotet

- Increased chances of getting infected with another malware  
→ Increased profits
- Strengthening the email sending infrastructure
- Increase in new attack targets (email addresses)

A mechanism that can specialize in increasing the number of infected hosts

→ Defenders need to reduce the number of infections

## 5.3. Purpose of attack groups using Emotet

- Malware that infects after Emotet (2019/09–)

malware	time	Infection
Ursnif	2019/09–10	only in Japan
Trickbot	2019/10–12, 2020/07–	also in Japan
Qakbot	2020/07–	also in Japan
Zloader	2020/09–	only in Japan
IcedID	2020/10–	not in Japan

- all banking trojan
- Attack groups will be different for each malware

## 5.4. Secondary infection malware by Emotet

- Secondary infection malware depends on the Geo Location of the IP at the time of infection
  - Secondary infection in the target country, no infection in non-target countries
- Malware that is secondarily infected only in Japan targets Japan
  - Ursnif, Zloader
- To reduce Emotet's attacks on Japan, it is also effective to block the purpose of attack groups targeting secondary infections.

## 5.4.1. Ursnif secondary infection from Emotet

- Ursnif(Dreambot), Trickbot via Emotet
  - Ursnif and Ursnif via Emotet have the same settings
  - Ursnif and Trickbot WebInjects URLs match  
→ Attack group is considered Ursnif-B

[See JSAC2020 presentation]

[https://jsac.ipcert.or.jp/archive/2020/pdf/JSAC2020\\_5\\_sajo-takeda-niwa\\_ip.pdf](https://jsac.ipcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_ip.pdf)

- This attack group is known to use an account called “Jer” in other reports

Ref: <https://medium.com/csis-techblog/the-end-of-dreambot-a-loved-piece-of-gozi-24cc9bfc8122>

## (Ref) Trickbot

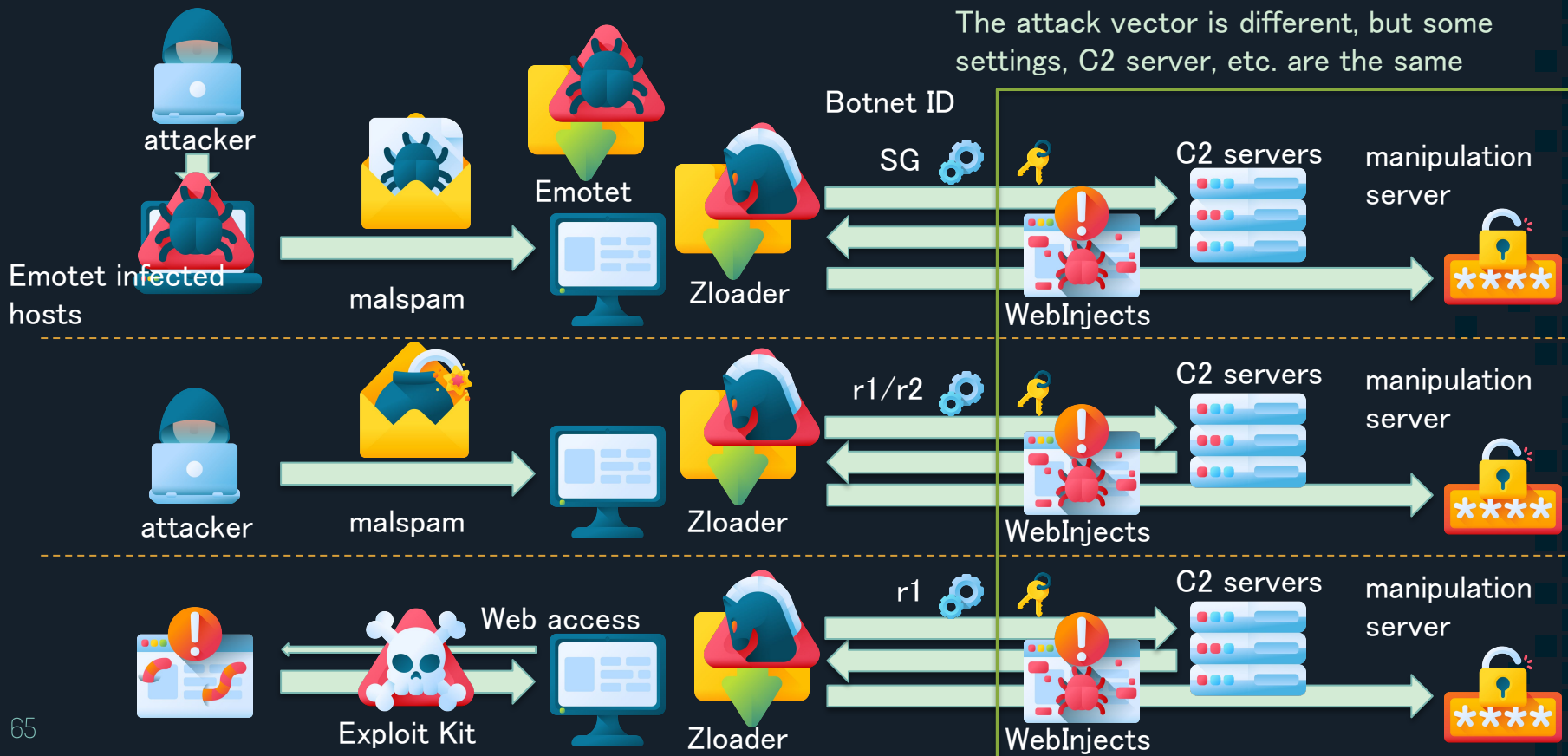
- Trickbot is used by various attack groups
    - Not all Trickbot distributions are via Emotet, and some Trickbot distributions via Emotet are Jer
  - WebInjects for Japan exists in one record group from October 15, 2019 to March 2020 (About 30% of the total)
    - This user is considered Jer
    - After 2020/03, most record groups including the above for Japan have been deleted from Trickbot's WebInjects.
- At the same time, Trickbot's attack group is said to have migrated to more sophisticated Bazaar malware.

## 5.4.2. Zloader secondary infection from Emotet

- Zloader
  - Observed only in Japan after 2020/09
  - Increased emails to Japan at the same time
- Zloader targeting Japan has 3 infection methods
  - Malware that infects after Emotet
  - Infection from malspam attached xls
  - Infection via Exploit-Kit
- 3 types of Zloader have the same config and C2
  - The same group is attacking
  - WebInjects targeting Japanese financial institutions



## 5.4.3. Zloader attack vector and settings



## 5.5. Relationship of secondary infection from Emotet

- Each Ursnif and Zloader attack group attempts to infect even without Emotet.
  - Emotet is just **one of the attack vectors**
- There are **similarities** between the two malware campaigns
  - email subject, body
  - Document design
  - WebInjects

## 5.5.1. Document design comparison

- Emotet's Japanese document and xlsb that infects Zloader have the same design, the image is the same hash
- Jer used almost the same image in the past
  - The image is mosaic due to hash modification

Emotet and zloader design



2018/12/28 Ursnif design



## 5.5.2. Comparison of email body

- The body of the Zloader malspam on 2020/10/14 is the same as the malspam body of Ursnif on 2017/06/13 – 2017/11/22.
- In addition, the body of Zloader malspam is the one used in the past in Jer's Ursnif malspam body.

### 2020/10/14 Zloader malspam

経理ご担当者様

いつも大変お世話になっております。  
株式会社ジャパントラストの佐々木です。

今月分のご入金より振込口座の変更をさせていただきたいのですが、  
ご対応可能でしょうか？

新たな振込先に関しましては、  
現在、手続き中で10月13日に完了予定となります。

本日中に仮のご請求書データをお送り致しまして  
手続き完了次第、正式なご請求書データをお送り致します。

急なご連絡になってしまい大変申し訳ございませんが、  
ご対応をいただけますと大変助かります。

### 2017/06/13 Ursnif malspam

経理ご担当者様

いつも大変お世話になっております。  
株式会社ジャパントラストの佐々木です。

今月分のご入金より振込口座の変更をさせていただきたいのですが、  
ご対応可能でしょうか？

新たな振込先に関しましては、  
現在、手続き中で6月15日に完了予定となります。

本日中に仮のご請求書データをお送り致しまして  
手続き完了次第、正式なご請求書データをお送り致します。

急なご連絡になってしまい大変申し訳ございませんが、  
ご対応をいただけますと大変助かります。

Ref: [https://www.jc3.or.jp/topics/vm\\_index.html](https://www.jc3.or.jp/topics/vm_index.html)  
<https://bomccss.hatenablog.jp/entry/2020/10/28/132546>

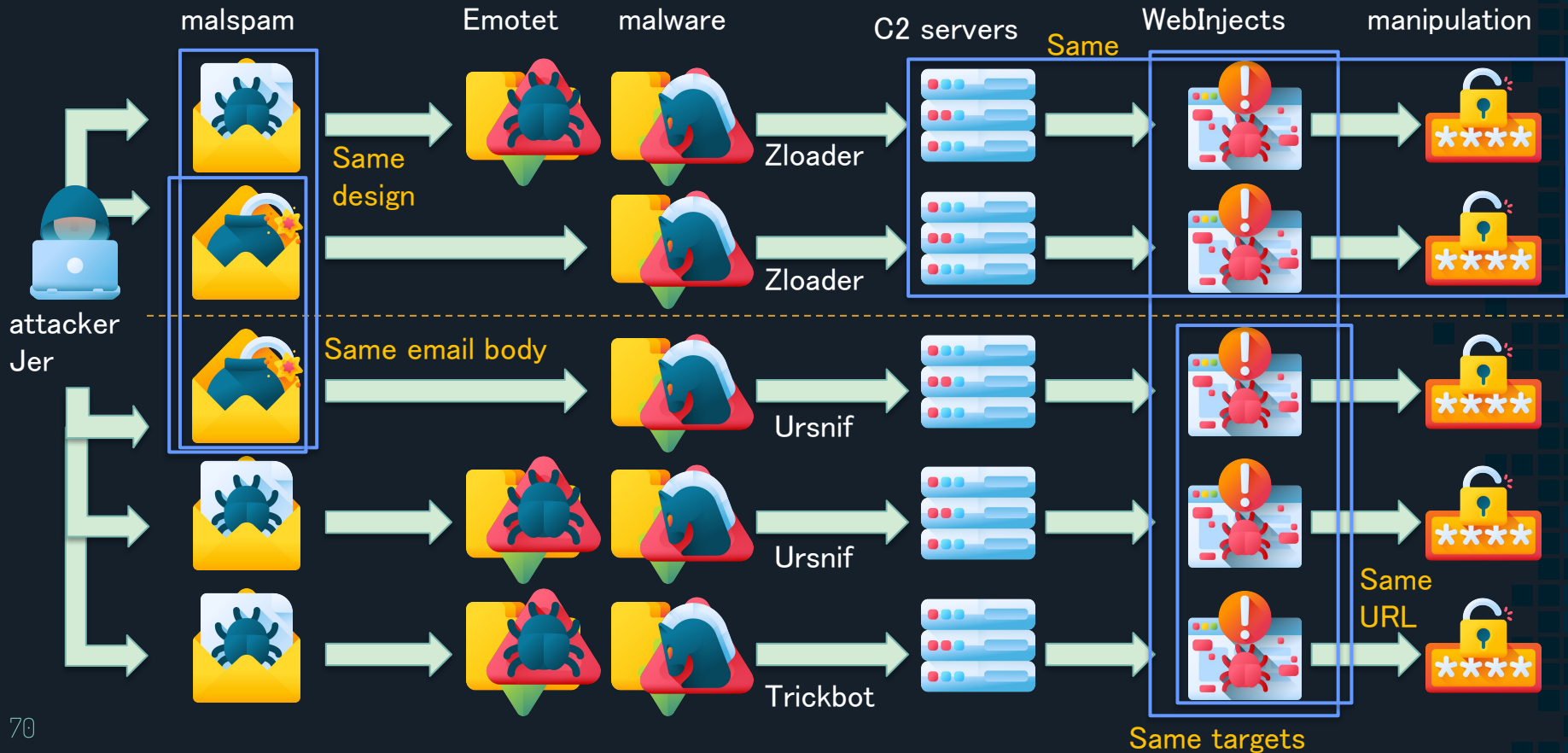
## 5.5.3. WebInjects

- Target of WebInjects
  - Ursnif and Zloader are mainly targeted at banks and credit card companies, and the target organizations are the same.
    - Zloader's WebInjects are frequently added and changed and are considered to be under continuous development.
- No other Web Injections for Japan targeting both banks and credit card companies
  - In the past Ramnit, Panda Banker targeted credit card companies
  - Some of Ursnif target Japanese banks

Ref: <https://blog.trendmicro.co.jp/archives/19291>

<https://www.botconf.eu/wp-content/uploads/2018/12/2018-J-Wyke-Tracking-actors-through-their-webinjects-.pdf>

## 5.5.4. Relationship between Zloader and Ursnif



## 5.6. Purpose of attack groups

- The purpose of the attack group that operates Emotet is financial profit, and spreading Emotet more will lead to profit.
- Ursnif and Zloader infected from Emotet are used by the same attack group
  - Aim for money with Banking Trojan
  - It may change to other malware, but it is likely that attacks will continue.
- Ransomware attacks via Emotet that occur overseas may not occur very often in Japan.

## 6. Countermeasures



Windows Update

### Some apps need to be updated

These programs need to be upgrade because they aren't compatible with this file format.

\* Microsoft Word

You need to click Enable Editing and then click Enable Content.



## 6. Countermeasures

- Keep your OS and software up to date
- Keep your antivirus software pattern files up to date
- Block emails aimed at infection
- Disable macro autorun in document files
- Prohibit communication to the outside by script
- Block communications using IoCs
  - Communication destination shared by [URLHaus](#)
  - IP address of C2 server shared by [feodo.tracker](#)
- Set up multi-factor authentication for your email account
- Restrict administrative shares
- Regular alerts with the latest information
  - Especially on Twitter, the latest information is shared
  - [paste.cryptolaemus.com](#)

## 7. Summary



## 7. Summary

- Explaining Emotet attack campaign targeting Japan
  - The Flow of attacks aimed at infection
  - Sharing the infection situation in Japan
  - Analysis attack groups that use Emotet

Attack campaigns targeting Emotet infections are changing rapidly, so use the latest TTPs and IoCs from Twitter and other sources as a proactive countermeasure.

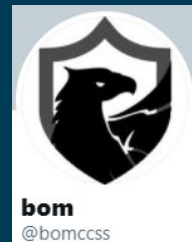
Let's all reduce Emotet infections.

# THANKS!

## Any questions?

### Work with Community

[@bomccss](#)



**bom**  
@bomccss

[@sugimu\\_sec](#)



**sugimu**  
@sugimu\_sec

[@abel1ma](#)



**abel**  
@abel1ma

[@waga\\_tw](#)



**わが**  
@waga\_tw

[@58\\_158\\_177\\_102](#)



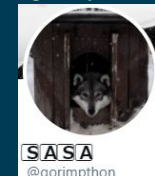
**moto\_sato**  
@58\_158\_177\_102

[@wato\\_dn](#)



**watoly**  
@wato\_dn

[@gorimphthon](#)



**SASA**  
@gorimphthon

[@papa\\_anniekey](#)



**hiro\_**  
@papa\_anniekey

[@satontonton](#)



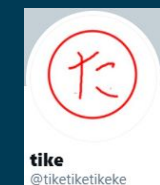
**さとお**  
@satontonton

[@catnap707](#)



**ねこさん** (ΦωΦ)  
@catnap707

[@tiketiketikeke](#)



**tike**  
@tiketiketikeke

[@autumn\\_good\\_35](#)



**Autumn Good**  
@autumn\_good\_35

[@00001B1A](#)



**\_roku**  
@00001B1A

[@AIR3\\_ytakeda](#)



**ytakeda**  
@AIR3\_ytakeda

[@tachi4439](#)



**tachi4439**  
@tachi4439

[@fumik0\\_](#)



**Fumik0\_**  
@fumik0\_

[@AES256bit](#)



**あゆむ**  
@AES256bit

[@romonlyht](#)



**ROMonlyHT**  
@romonlyht

[@sepi140](#)



**kuma**  
@sepi140

[@anemone\\_fish](#)



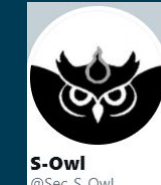
**Tamperer**  
@anemone\_fish

[@ozuma5119](#)



**Osumi, Yusuke**  
@ozuma5119

[@Sec\\_S\\_Owl](#)



**S-Owl**  
@Sec\_S\_Owl