

JPCERT Coordination Center official Blog

 blogs.jpcert.or.jp/en/2019/12/emotetfaq.html



佐條 研(Ken Sajo)

December 4, 2019

How to Respond to Emotet Infection (FAQ)

Emotet

-
- 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.jpcert.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.

We have been informed of emails impersonating someone. What can we do?

When suspicious email impersonating someone with an attachment is received, it is possible that either of the following events has occurred:

- A) The device that uses the sender's account is infected with Emotet, and information about emails and contact list have been stolen.
- B) Partners and users (with whom you have exchanged emails) have been infected with Emotet, and their contact list has been stolen. (The recipients of the malicious email have not been infected with Emotet, but the email address has been added to the lists of recipients.)

If the email referring to an actual message body (Figure 1) is received, the device that uses the sender's email account is likely to be infected (case A).



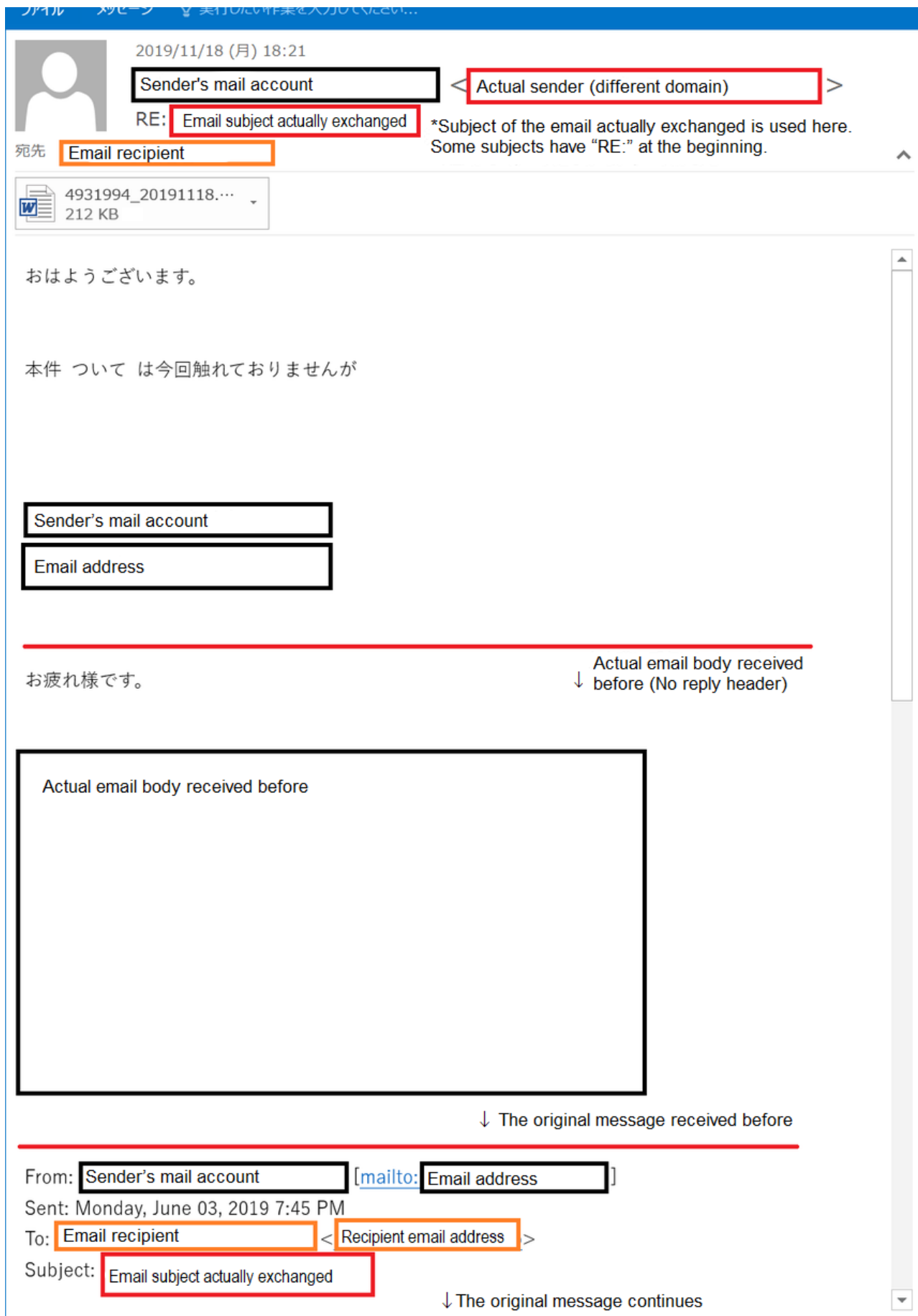


Figure 1 : Example of Emotet email in reply to an existing thread (A)

In case of an email as in Figure 2, it is assumed that the email is auto-generated to disguise itself as a reply to a thread. Both A) and B) can apply to this case, and it is unclear whether the device that uses the email account is infected or not.



Figure 2 : Example of email disguising as a reply (B)

What can we do to check whether we are infected with Emotet or not?

(Updated on 6 February, 2020)

JPCERT/CC released a tool “EmoCheck” to check whether a device is infected with Emotet. See below for instruction.

1. Check Emotet infection with EmoCheck

1-1.Download EmoCheck

Please download EmoCheck from the following website and copy it to the device that is suspected of being infected. Please choose emocheck_x86.exe or emocheck_x64.exe depending on the device. (If you are not sure which to use, choose emocheck_x86.exe.)

JPCERTCC/EmoCheck - GitHub

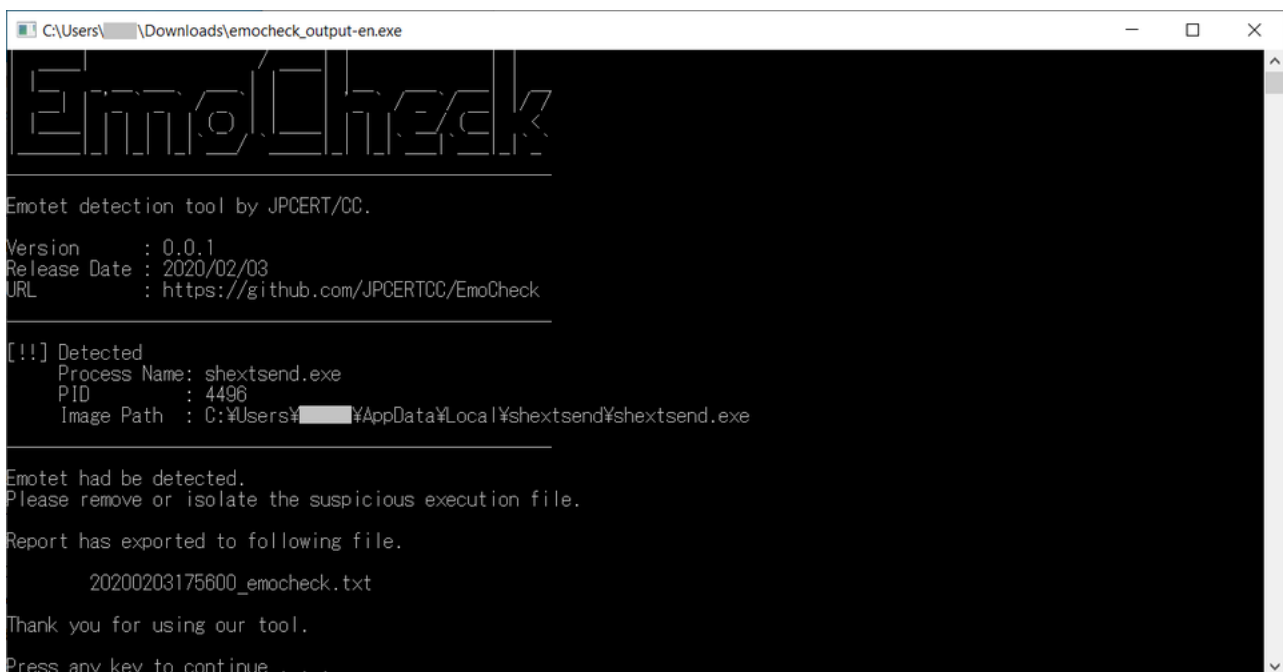
<https://github.com/JPCERTCC/EmoCheck/releases>

1-2.Execute EmoCheck

Execute the tool using the Command Prompt or PowerShell.

(Note: If you execute the program by double-clicking, it will be blocked by Windows Defender Smart Screen as it does not have a Code Signing Certificate. We are now working to rectify the issue in the next release.)

If you see the message “[!!] Detected” as follows, your device is infected with Emotet.



```
C:\Users\...Downloads\emocheck_output-en.exe
EmoCheck
Emotet detection tool by JPCERT/CC.
Version      : 0.0.1
Release Date : 2020/02/03
URL          : https://github.com/JPCERTCC/EmoCheck

[!!] Detected
Process Name: shextsend.exe
PID         : 4496
Image Path  : C:\Users\...\AppData\Local\shextsend\shextsend.exe

Emotet had be detected.
Please remove or isolate the suspicious execution file.
Report has exported to following file.
          20200203175600_emocheck.txt

Thank you for using our tool.
Press any key to continue . . .
```

Figure 5: Emotet infection detected by EmoCheck

The result is also exported in .txt file in the folder where EmoCheck was executed.

```
20200203175600_emocheck.txt - Notepad
File Edit Format View Help
[[Emocheck v0.0.1]
Scan time: 2020-02-03 17:56:00

-----

[Result]
Detected Emotet process.

[Emotet Process]
  Process Name   : shextsend.exe
  Process ID    : 4496
  Image Path     : C:\Users\████████\AppData\Local\shextsend\shextsend.exe

-----

Please remove or isolate the suspicious execution file.

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

Figure 6: Emotet result output

If you see the message “No detection.”, your device is not infected with Emotet.

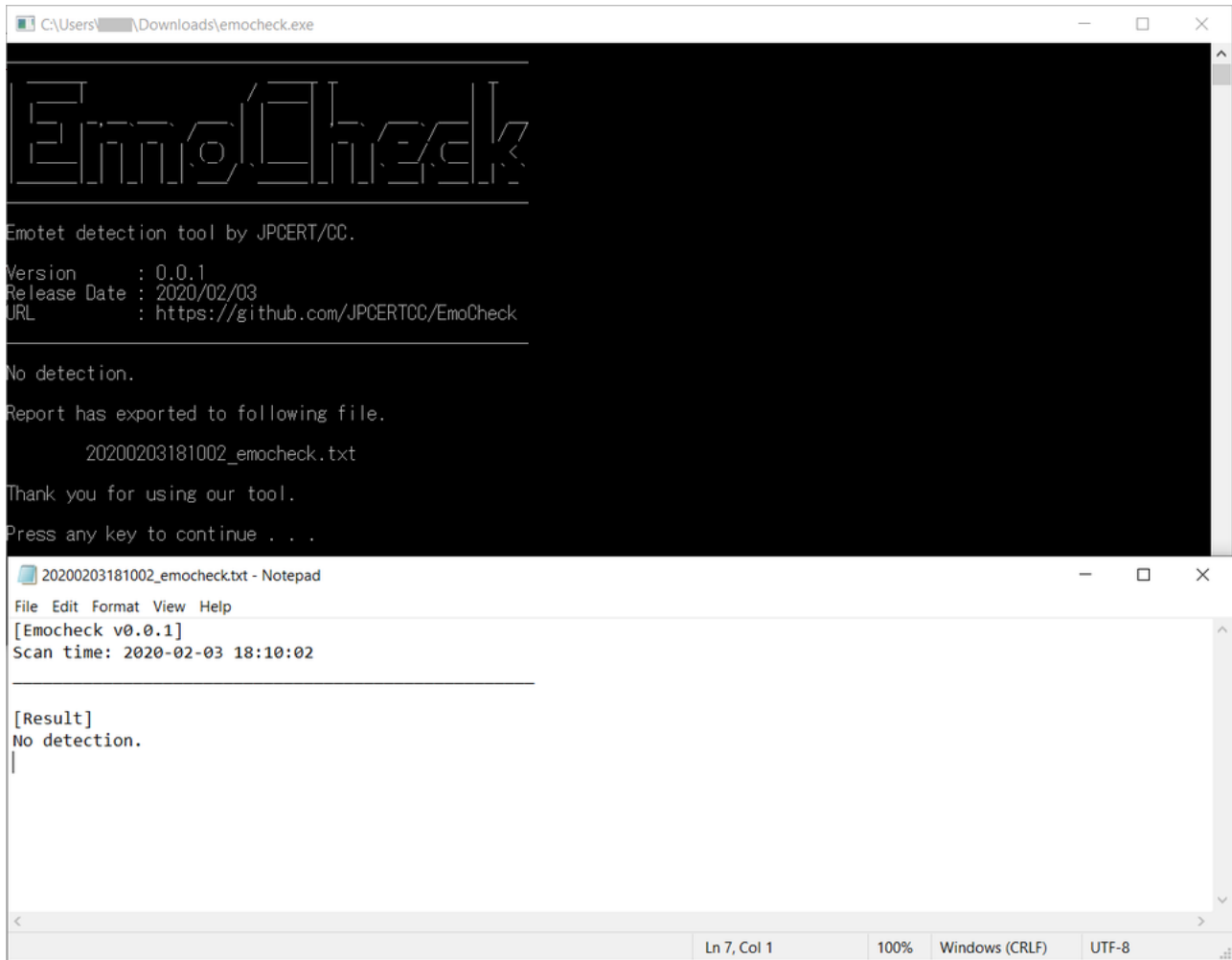


Figure 7: Emotet infection not detected

1-3. How to deal with the infection

If an infection has been found in your environment, you can deactivate the malware by either of the following ways:

On Explorer, open the “image path” folder which is shown in the EmoCheck result and delete the executable file in the folder.

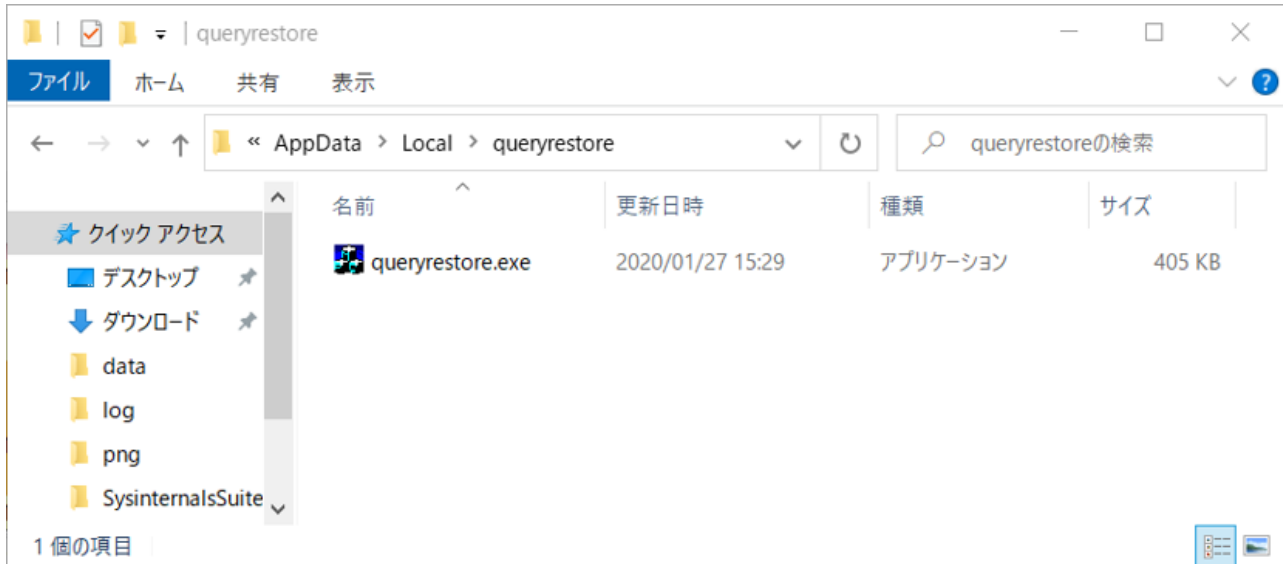


Figure 8: Image path that stores Emotet (example)

Launch Task Manager, and in the “details” tab, choose the process ID which corresponds to the process shown in the EmoCheck result. Click “End Process”.

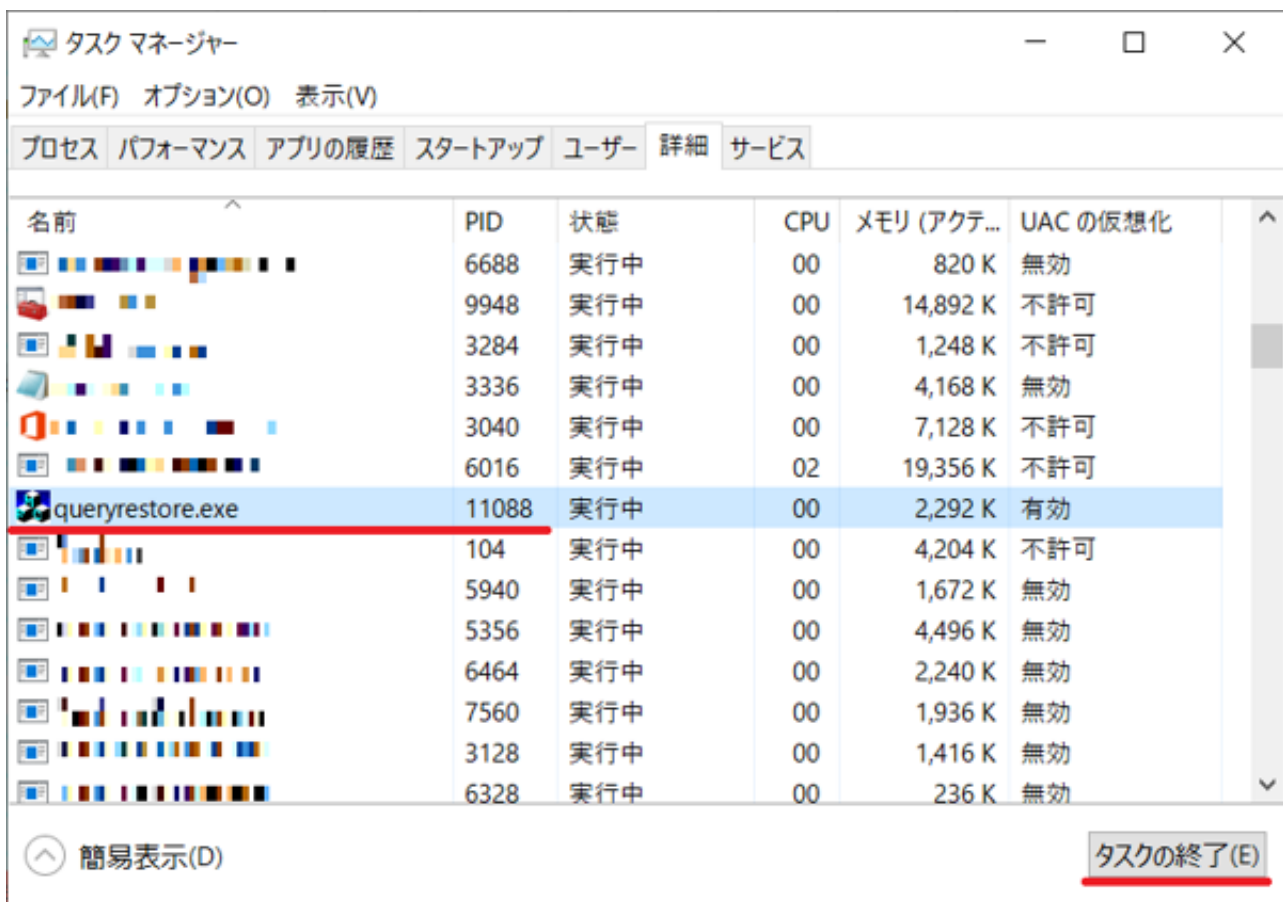


Figure 9: Choose Process ID

If you are not able to confirm Emotet infection with EmoCheck, please follow the below instruction to confirm.

1. Confirm with the impersonated person

Check whether the person opened the suspicious attachment and saw the messages in the sample screenshots (See Reference “The screenshots of the attached Word file”). If they have seen one of the messages, check whether the macro is enabled on their device. If the macro is enabled, it is possible that the device is infected with malware.

2. Perform the scan with anti-virus software

Perform device scan with the latest anti-virus signatures.

*Emotet has many variants, and even the latest signatures may not be able to detect infection for a few days. No detection does not necessarily mean no infection. It is recommended to update the signatures and conduct the scan regularly.

3. Check auto-start settings

Emotet has several methods for maintaining persistence such as setting auto-start registry keys, save the payload into Startup folder, etc.

Check the following settings and confirm that suspicious file or setting does not exist.

[Typical Windows OS auto-start settings]

- Auto-start registry [*1]
- Task Scheduler
- Service
- Startup folder

(*1) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

[Folders that Emotet is likely to be located]

- Folders under C:\Users(username)\AppData\Local\
- C:\ProgramData\
- C:\Windows\system32\
- C:\
- C:\Windows
- C:\Windows\Syswow64

*If there is a suspicious executable file under C:\ProgramData\ that is registered in the Task Scheduler, it is likely that the device is also infected with Trickbot.

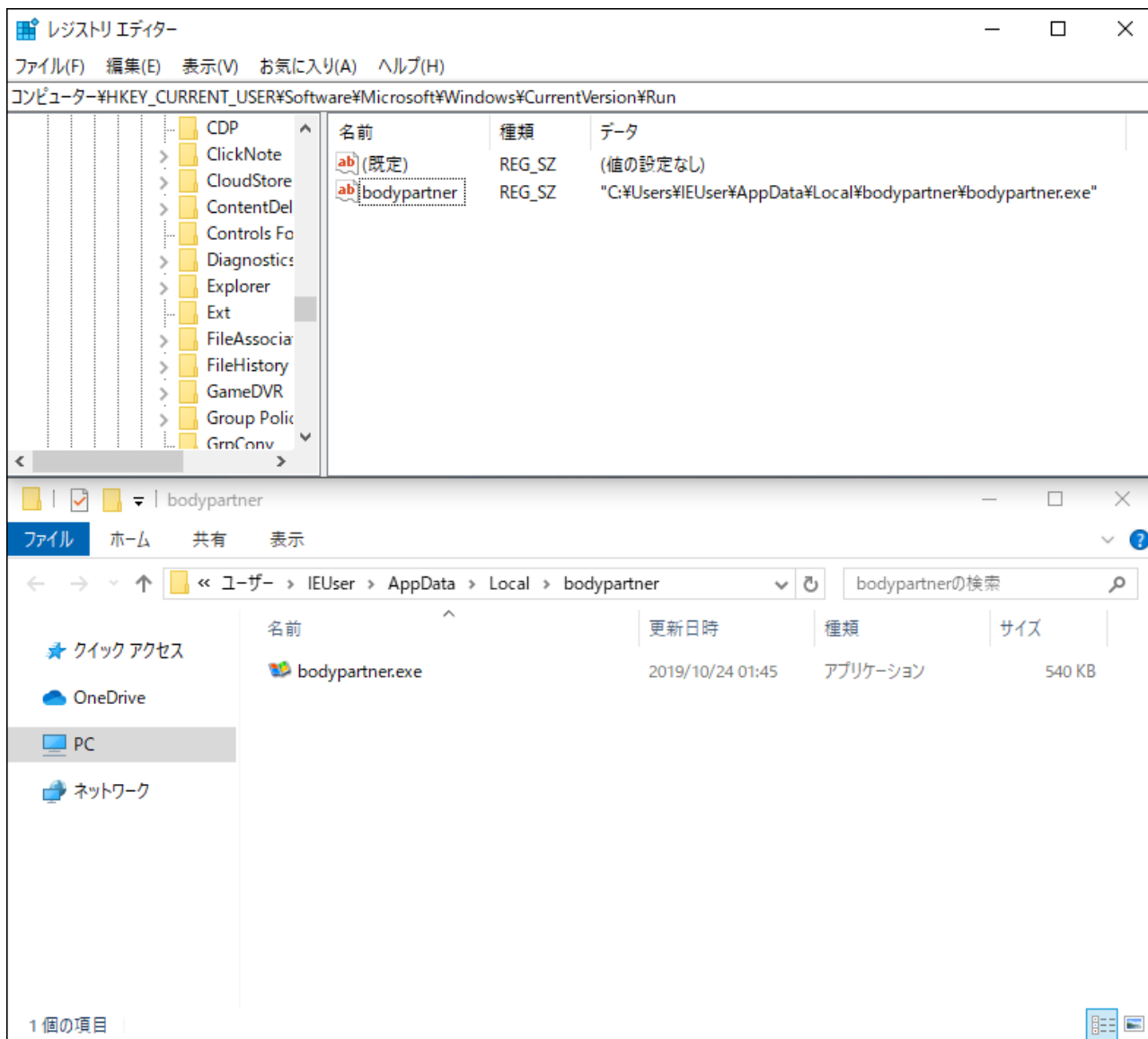


Figure 3: Example of Emotet registered in the Auto-start Registry [*1]
 (*Folder names and executable file names are randomly created for each device.)

4. Check email server log

Check the following points in your email server logs:

- High volume of impersonating emails whose HeaderFrom and EnvelopFrom do not match
- Unusual increase in the volume of outbound emails
- High volume of emails with a Word file attachment

5. Check network traffic log

If you record/monitor outbound communication, check proxy and firewall logs for any suspicious access to multiple ports (C&C server) from a single device.

[Example of ports that Emotet uses]

20/TCP, 22/TCP, 80/TCP, 443/TCP, 446/TCP, 447/TCP, 449/TCP, 465/TCP, 7080/TCP, 8080/TCP, 8090/TCP etc.

No.	Destination	Protocol	host	Info
7		HTTP	130:8080	POST /tlb/ HTTP/1.1 (application/x-www-form-urlencoded)
21		HTTP	79:8080	POST /raster/ HTTP/1.1 (application/x-www-form-urlencoded)
34		HTTP	217:8080	POST /enabled/attrib/ HTTP/1.1 (application/x-www-form-urlencoded)
43		HTTP	87	POST /walk/vermont/ HTTP/1.1 (application/x-www-form-urlencoded)
83		HTTP	27:8080	POST /cone/ HTTP/1.1 (application/x-www-form-urlencoded)
95		HTTP	101:8080	POST /results/dma/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
104		HTTP	220	POST /entries/ HTTP/1.1 (application/x-www-form-urlencoded)
118		HTTP	191:8080	POST /jit/balloon/ringin/ HTTP/1.1 (application/x-www-form-urlencoded)
126		HTTP	138:8080	POST /teapot/health/ HTTP/1.1 (application/x-www-form-urlencoded)
136		HTTP	8080	POST /dma/site/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
147		HTTP	13:8080	POST /taskbar/pnp/ HTTP/1.1 (application/x-www-form-urlencoded)
157		HTTP	188:8080	POST /site/walk/ringin/ HTTP/1.1 (application/x-www-form-urlencoded)
166		HTTP	136:8080	POST /odbc/json/ HTTP/1.1 (application/x-www-form-urlencoded)
204		HTTP	30:443	POST /codec/window/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
218		HTTP	93:8080	POST /arizona/enabled/ringin/ HTTP/1.1 (application/x-www-form-urlencoded)
272		HTTP	88	POST /entries/between/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
289		HTTP	26:8080	POST /prep/ HTTP/1.1 (application/x-www-form-urlencoded)
305		HTTP	16:8080	POST /between/ HTTP/1.1 (application/x-www-form-urlencoded)
325		HTTP	5:443	POST /json/guids/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
340		HTTP	70	POST /walk/symbols/ringin/merge/ HTTP/1.1 (application/x-www-form-urlencoded)
357		HTTP	150:8080	POST /ban/forced/ HTTP/1.1 (application/x-www-form-urlencoded)
368		HTTP	77:8080	POST /psec/arizona/ringin/ HTTP/1.1 (application/x-www-form-urlencoded)
379		HTTP	217:8080	POST /enabled/loadan/ HTTP/1.1 (application/x-www-form-urlencoded)

Figure 4 : C&C communication by Emotet (*Destination IP differs by sample)

What can we do when we find Emotet infection?

1. Isolate the infected device, preserve evidence and investigate affected area
 - Preserve evidence of the infected device
 - Check the emails stored in the device and email addresses in the contact list (These may have been leaked)
2. Change password of email accounts etc. used in the infected device
 - Email accounts used in Outlook and Thunderbird
 - Credentials stored in Web browsers
3. Investigate all devices in the network to which the infected device was connected

Check other devices in the network as the malware is capable of spreading infection by lateral movement

The following TTPs have been confirmed for lateral movement:

 - Leverage SMB vulnerability (EternalBlue)
 - Log on to Windows network
 - Use Administrative share
 - Register services
4. Monitor network traffic log

Make sure that the infected device is isolated and check whether there is any other infected device

5. Check other malware infection

Check whether the infected device is also infected with other types of malware as Emotet is capable of infecting the device with other types of malware. If this happens, further investigation and response is required.

- Some victims in Japan have also been infected with banking trojans such as Ursnif and Trickbot
- Victims overseas were also found infected with targeted ransomware

6. Alert stakeholders who may also be affected (whose email addresses have been stolen by the attacker)

Emails and email addresses in the contact list in the case A

Issue a press release if a wide range of stakeholders may be affected.

7. Initialise the infected device

How can we stop emails being sent from stolen accounts?

If emails and email addresses are stolen as a result of Emotet infection, impersonating emails with a malicious attachment will be sent continuously. Information of the stolen email addresses (message body and contact lists) are collected in the attack infrastructure, and this is used to distribute malware-attached emails. There is no way to stop emails from being sent.

It is likely that the recipients will continue to receive malware-attached emails repeatedly or impersonating emails will be sent to the stolen contacts. Please beware not to open suspicious email attachments. It is also recommended to perform the scan with the latest anti-virus signatures and make sure that your OS and software are running with the latest security updates.

What impact is expected if a device is infected with Emotet?

Emotet infection leads to exfiltration of emails and email addresses. Credentials stored in Web browsers can be harvested. It is also possible that the infection spreads to other devices in the network and that devices are at the risk of being infected with other types of malware such as banking trojans and ransomware.

What can we do to prevent Emotet infection?

Please refer to JPCERT/CC's security alert for details.

Alert Regarding Emotet Malware Infection

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

(Reference) “The screenshots of the attached Word file”

Since October 2019, the following 6 types of Word files leading to Emotet infection have been observed.

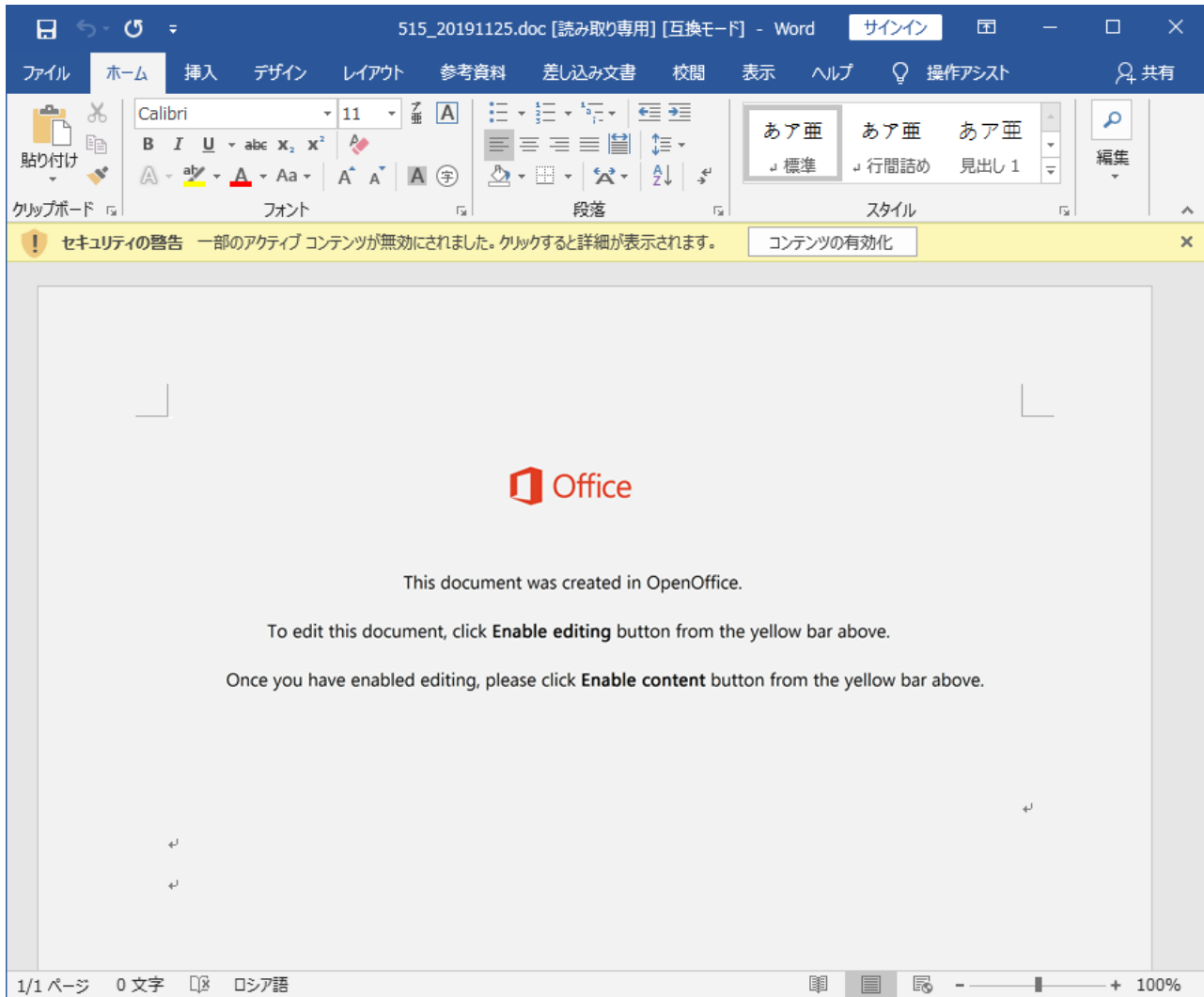


Figure 5 : Attached file example 1 (since 2019/11/26)

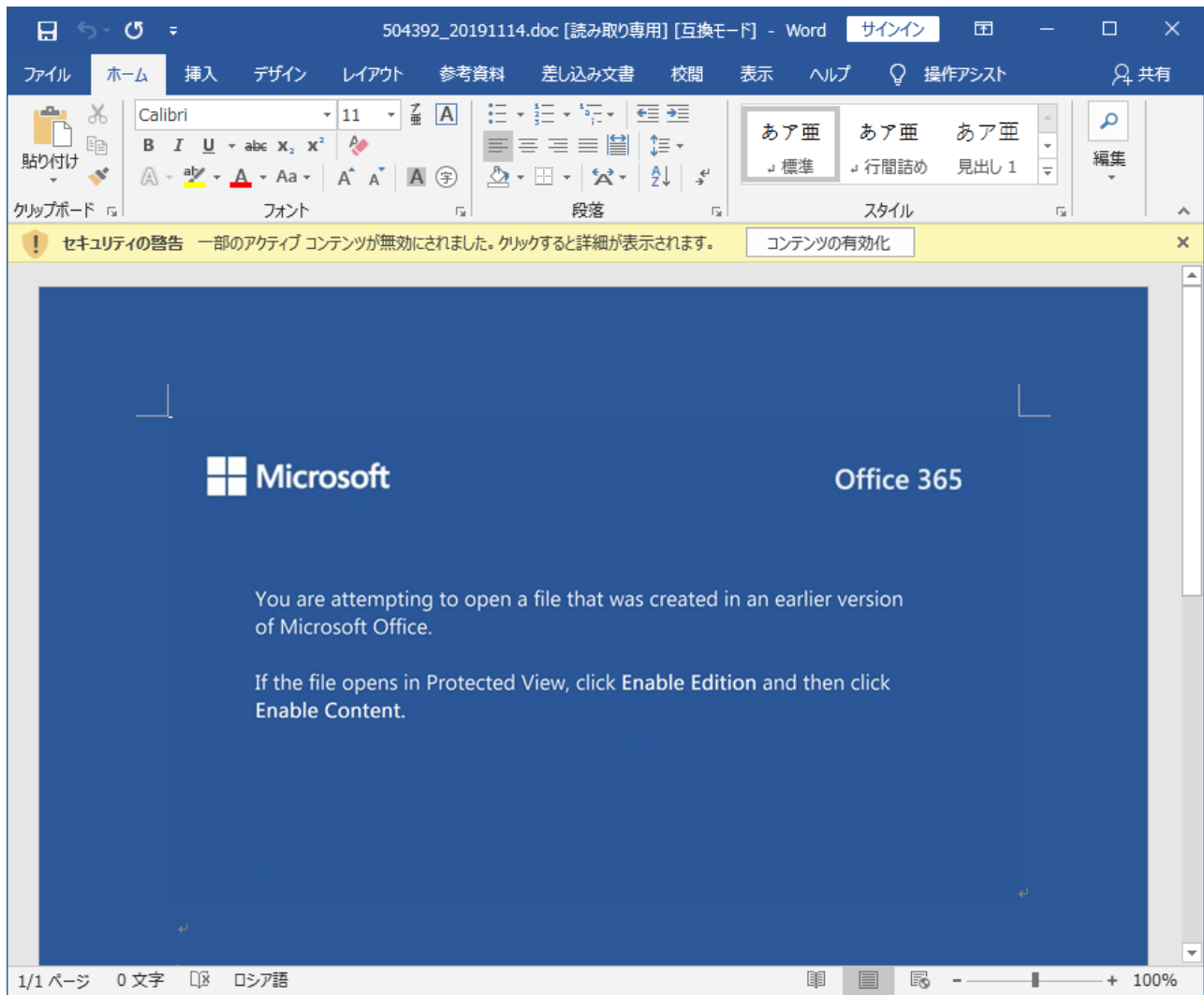


Figure 6 : Attached file example 2 (since 2019/10/30)

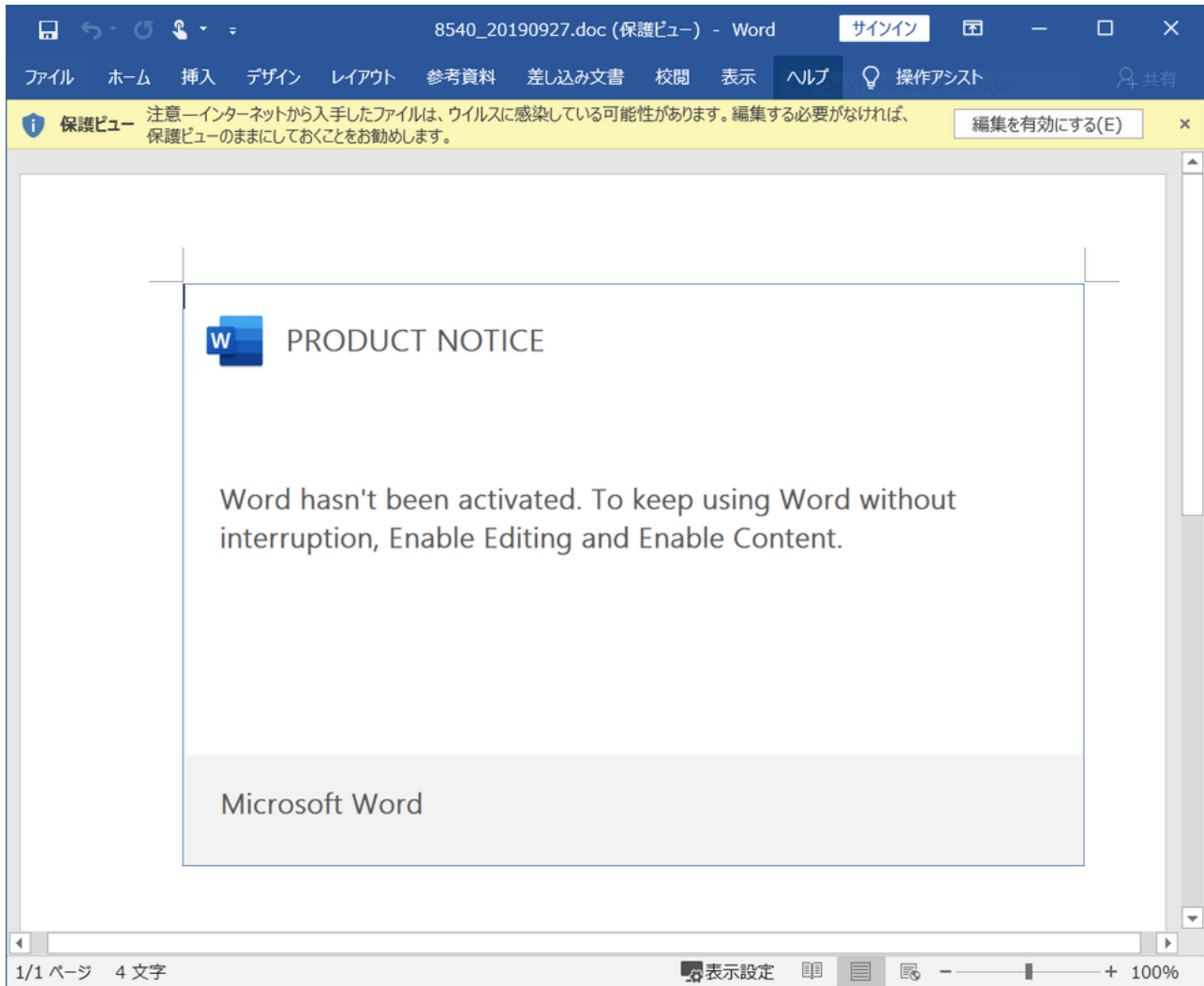


Figure 7 : Attached file example 3

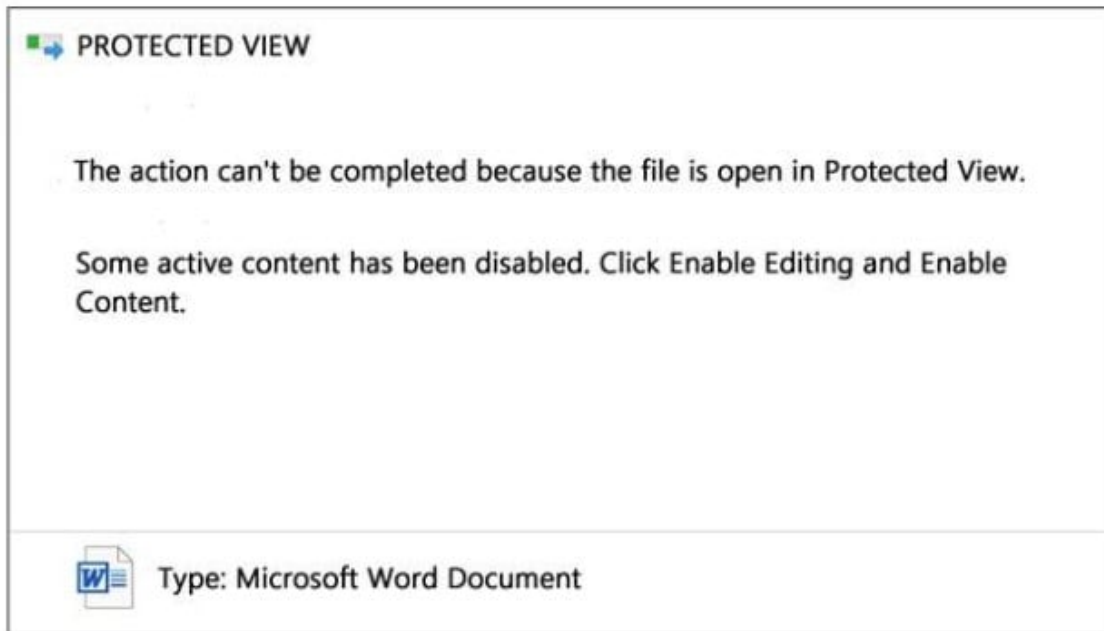


Figure 8 : Attached file example 4

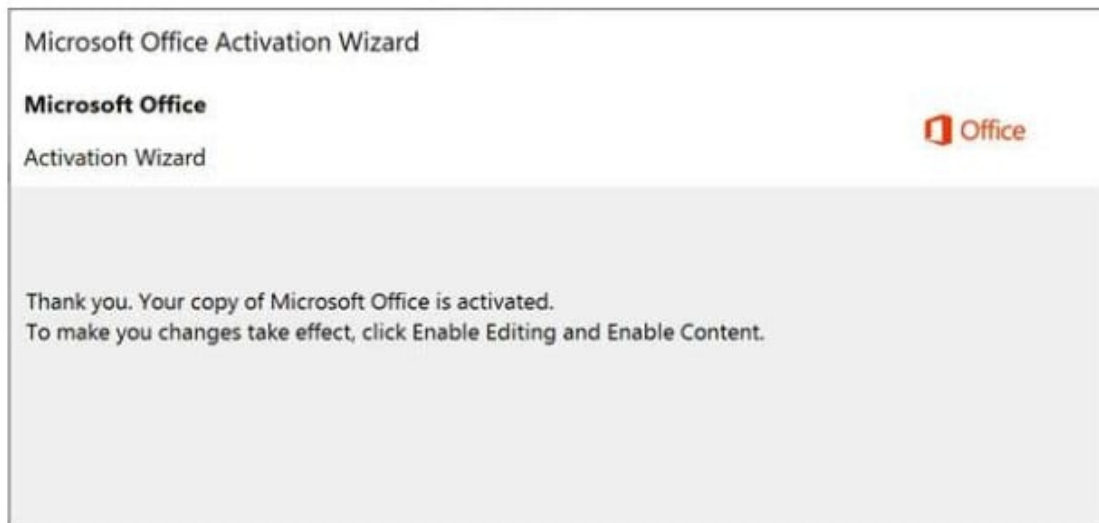


Figure 9 : Attached file example 5



Figure 10 : Attached file example 6

- Ken Sajo

(Translated by Yukako Uchida)

-
- [Email](#)

Author



佐條 研(Ken Sajo).

Joined JPCERT/CC in January 2019 after being engaged in security monitoring operation at a financial institution. Currently in charge of threat analysis and incident response for email scam and APT.

Was this page helpful?

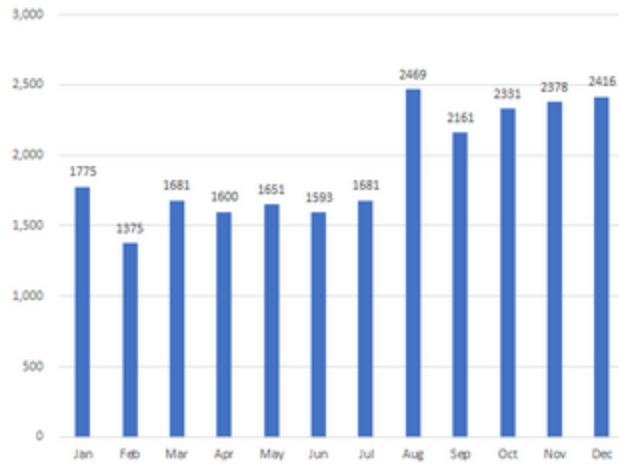
0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

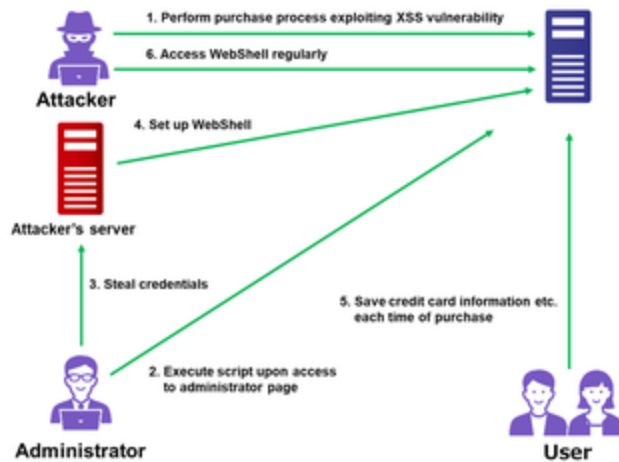
This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

Related articles



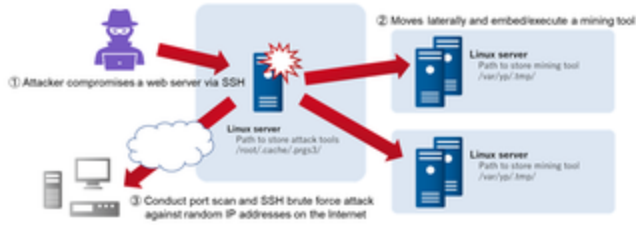
Trends of Reported Phishing Sites and Compromised Domains in 2021



Attack Exploiting XSS Vulnerability in E-commerce Websites



PHP Malware Used in Lucky Visitor Scam



Attacks Embedding XMRig on Compromised Servers

```

v7 = mal_check_count(http_strc->URL);
(*void __stdcall __)(int, int, int, int __)o_InternetCrackur1A[0])(http_strc->URL, v7,
if ( v4 == 1 )
{
  wsprintfA(
    &v3,
    "Content-Type: multipart/form-data; boundary=%s\r\n",
    (const char *)http_strc->http_bonday_str);
  if ( !v20 || !v21 )
  {
    if ( v20 )
    {
      wsprintfA(
        &v32,
        "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name1,
        (const char *)http_strc->http_body_text);
    }
    else
    {
      wsprintfA(
        &v32,
        "--%s\r\n"
        "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
        "Content-Type: image/png\r\n"
        "\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name,
        (const char *)http_strc->http_filename);
    }
  }
  else
  {
    wsprintfA(
      &v32,
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"\r\n"
      "\r\n"
      "%s\r\n"
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
      "Content-Type: image/png\r\n"
      "\r\n",
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name1,
      (const char *)http_strc->http_body_text,
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name,
      (const char *)http_strc->http_filename);
  }
  wsprintfA(&v33, "%s\r\n--%s\r\n", (const char *)http_strc->http_bonday_str);
  v27 = mal_check_count((int)&v32);
  v28 = mal_check_count((int)&v33);
}

```

Lazarus Attack Activities Targeting Japan (VSingle/ValeforBeta)

[Back](#)

[Top](#)

[Next](#)