

Emotet Disruption and Outreach to Affected Users - JPCERT/CC Eyes

By 佐條 研(Ken Sajo)

Published: 2021-02-24 · Archived: 2026-04-05 14:28:12 UTC

- [Emotet](#)

Since October 2019, many cases of Emotet infection were reported. JPCERT/CC has published [a security alert](#) and [a blog article](#) detailing the detection and security measures, as well as providing notification and support for affected users.

Europol announced that Emotet infrastructure was disrupted thanks to the joint operation together with some foreign authorities in January 2021 and information regarding affected users is to be distributed via the CERT network. In Japan, there are still many infected devices, and JPCERT/CC has been notifying those affected with the support from local and international partners.

This article explains the global operation for Emotet disruption and the changes in the number of infected devices in Japan since then, followed by the notification activity by JPCERT/CC and guidance on how to respond to the infection.

Contents

- [1. Emotet overview](#)
- [2. Emotet disruption](#)
- [3. Emotet infection in Japan](#)
- [4. Notification to affected users](#)
- [5. Response to infection](#)
- [6. Updates on our notification activities](#)

1. Emotet overview

A device is infected with Emotet when a user opens a malicious Word file and selects “Enable content”. The malware may perform the following on the infected devices:

- Steal credentials stored in the device or browsers
- Use the stolen credentials to spread infection in the network via SMB
- Steal Email accounts and passwords
- Steal Email contents and contact information
- Send emails to spread infection using the stolen Email accounts and contents etc.
- Infect the device with other kinds of malware

2. Emotet disruption

Emotet’s infrastructure was disrupted on 27 January 2021 as a result of “Operation LadyBird”, which is a joint effort by the authorities in [the Netherlands](#), [Germany](#), [the United States](#), [the United Kingdom](#), France, Lithuania, [Canada](#) and [Ukraine](#), coordinated by [Europol](#) and [Eurojust](#). The following is the achievement of this operation:

- C2 servers connected to Emotet are now under the control of the authorities
- Some members operating Emotet have been arrested
- Infected devices are now redirected to servers controlled by the authorities

Thanks to this operation, it is safe to say that Emotet is no longer harmful. Nonetheless, infected devices are still likely at the risk.

3. Emotet infection in Japan

Following the joint operation, foreign partner organisations started providing JPCERT/CC with the information about infected hosts in Japan, particularly the details of the devices connected to the servers that are under the foreign authorities’ control. Figure 1 shows the number of infected devices in Japan based on the data provided.

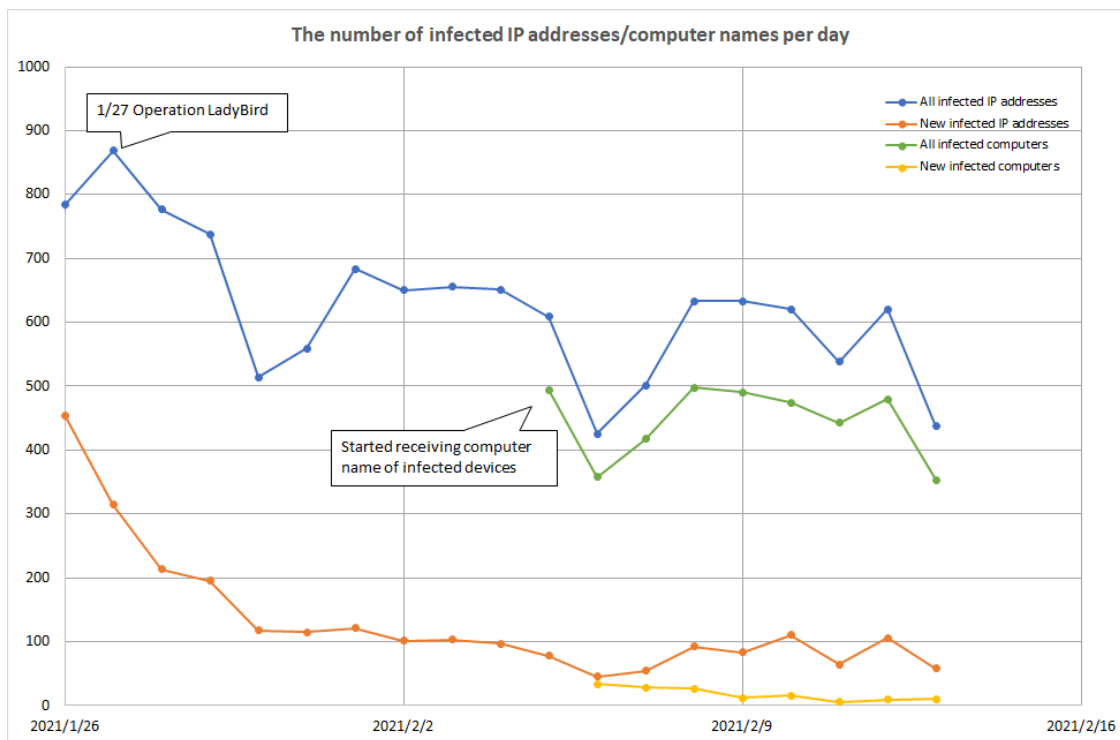


Figure 1 : Emotet Infected devices in Japan

As of 27 January, when the joint operation took place, there were connections to the infrastructure from about 900 IP addresses in Japan. Starting on 5 February, we have also been receiving the computer name of the infected devices. It is assumed that the number of the unique computer names indicates more accurate number of infected devices, as an IP address linked to a device may change.

With the disruption of the infrastructure, Emotet’s anti-detection function will no longer work, and it will be detected and/or removed by antivirus software instead. However, based on the number of the computer names, it is assumed that there are about 500 infected devices as of February 2021.

4. Notification to affected users

Based on the information provided by the relevant parties, JPCERT/CC has been notifying the users of the infected devices in Japan with the support of ISPs and other partners.

On 19 February, Japan’s Ministry of Internal Affairs and Communication, together with the National Police Agency, ICT-ISAC and ISPs, announced their joint effort on notification activities to users of infected devices based on the information from foreign authorities. While cooperating in this initiative, JPCERT/CC will also continue the aforementioned outreach activities based on the information from partners.

Thanks to the global operation, Emotet will be uninstalled from the devices at 12:00 on 25 April 2021 (according to the local time of each device). However, security measures still need to be implemented on the infected devices as the malware may have already performed the following:

- Steal credentials stored in the device or browsers
- Steal Email accounts and passwords
- Steal Email contents and contact information
- Infect the device with other kinds of malware

Users still need to take measures if antivirus software has detected and/or removed Emotet.

5. Response to Emotet infection

“EmoCheck”, developed by JPCERT/CC, can be used to check if a device is infected with Emotet. Please download the tool from GitHub and copy it to the devices that need checking. It is recommended to run it with the privilege of the user who normally use the device.

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

If the message “Emotet was detected” is displayed (as highlighted in red in Figure 2), the device is infected with Emotet.

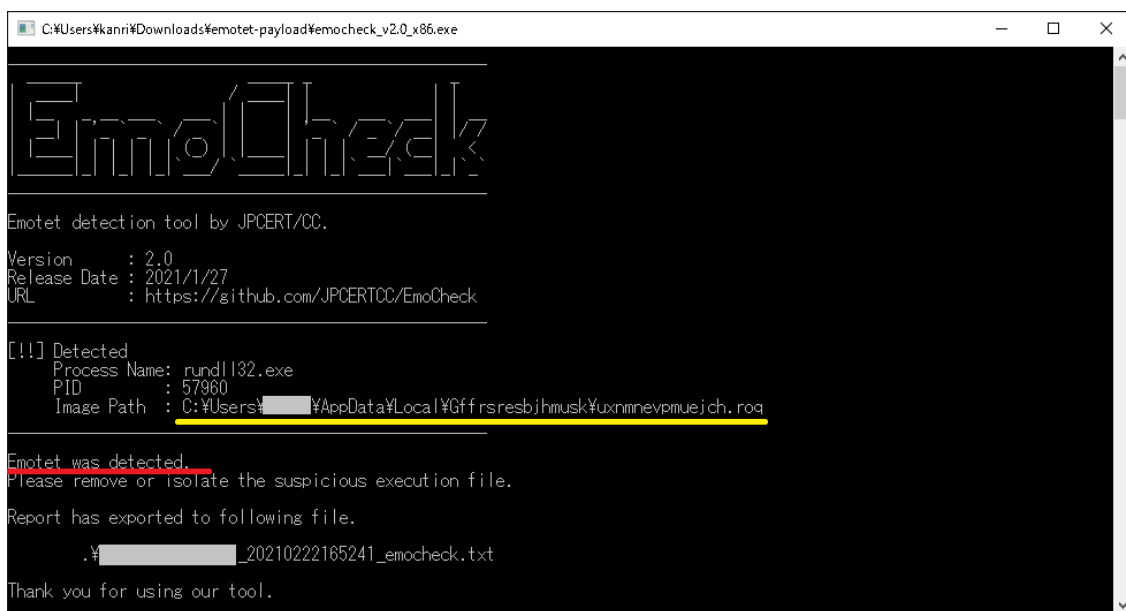


Figure 2 : Sample results (Emotet detected)

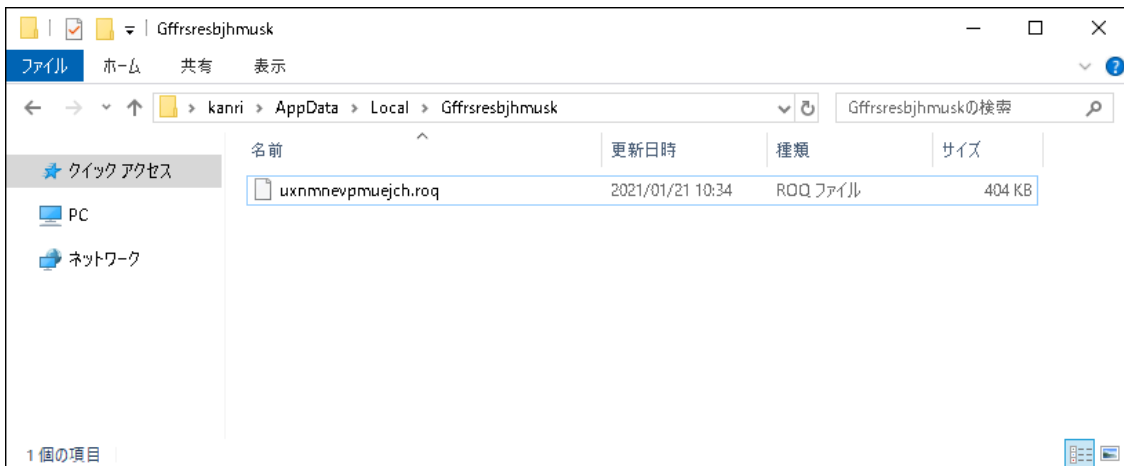


Figure 3 : Sample image path of Emotet according to EmoCheck result (highlighted in yellow in Figure 2)

When the infected devices are identified, please take the following security measures:

- Delete Emotet which is stored in the image path according to the EmoCheck result.
- Change email account passwords for Outlook, Thunderbird, etc.
- Change passwords stored in browsers.
- Check if the device is infected with other kinds of malware.

If the device is infected with other kinds of malware, evidence may be left in the following locations:

- Autorun registry
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- Task scheduler

If the above settings refer to the suspicious folders as below, the device is possibly infected with other kinds of malware:

- Folders under C:\Users(user name)\AppData\
C:\ProgramData\

More details on how to check and respond to the infection are also available on [our past blog article](#)

6. Updates on our notification activities (Updated on 25/May 2021)

JPCERT/CC has notified affected users cooperating with ISPs and other organizations since we received the said data in late January until Emotet was automatically deleted in late April. Through the joint notification effort by the National Police Agency and the Ministry of Internal Affairs and Communication, the information on the affected IP addresses was provided to ICT-ISAC in mid-February and received by each ISP in late March. This accounts for about 90 percent of the whole affected IP addresses in Japan, and JPCERT/CC has notified the rest directly to administrators since late January.

After the global take down operation, Emotet was updated so that it automatically stops itself at 12:00 on 25 April (local time of each device). The following figure on the number of Emotet-infected devices in Japan clearly shows

that only few infections have been observed since then.

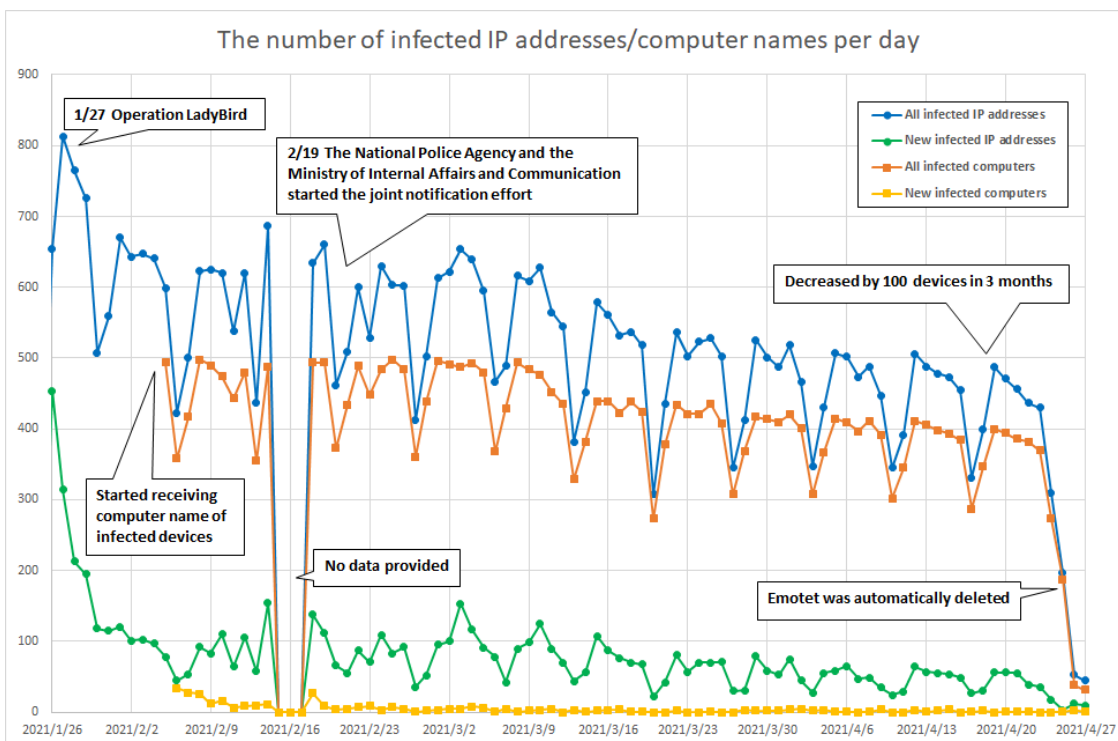


Figure 4 : Emotet Infected devices in Japan

We appreciate all the supports we received from everyone concerned.

In closing

We would like to take this opportunity to thank the effort by “Operation LadyBird” in disrupting the Emotet infrastructure.

Besides Emotet, there are many other kinds of malware spreading infection via email and its attachment. Please pay careful attention when you open attachments. We also recommend that you regularly scan your devices with the latest antivirus definition file, in addition to applying the latest security programs for your OS and software.

JPCERT/CC will continue to work closely with both local and international partners.

Ken Sajo

(Translated by Yukako Uchida)



[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.

Related articles



[Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise](#)

```

*key = 0x327C408;
*key[4] = 0x01583C2;
*key[8] = 0x0472834;
*key[12] = 0x0007708;
*key[16] = 0x1474421;
*key[20] = 0x4885A48;
*key[24] = 0x3078829;
*key[28] = 0x0200047;

v4 = m_ret_argloffset0x358(a1 + 3);
if ( !((2->CryptAcquireContext)(a1, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 0x1E, 0xF000000) )
return 0;
v3 = m_ret_argloffset0x358(a1 + 3);
handLehashob = a1 + 3;
if ( !((v3->CryptCreateHash)(*a1, 0x0004, 0, 0, a1 + 3) )
{
LABEL_0:
if ( *a1 )
return 0;
v6 = m_ret_argloffset0x358(a1 + 3);
(v6->CryptReleaseContext)(*a1, 0);
return 0;
}
if ( !CryptHashData(*handLehashob, key, 16u, 0)
|| (v8 = m_ret_argloffset0x358(a1 + 3));
v9 = a1 + 2;
!(v8->CryptDeriveKey)(*a1, 0x0004, *handLehashob, 0x000000, a1 + 2) )// CBC_AES_128
{
if ( *handLehashob )
{
v5 = m_ret_argloffset0x358(a1 + 3);
(v5->CryptDestroyHash)(*handLehashob);
}
goto LABEL_0;
}
v10 = m_ret_argloffset0x358(a1 + 3);
(v10->CryptSetKeyParam)(*v9, 3, 0x0001, 0); // OP_PADDING = PKCS40/7
v11 = m_ret_argloffset0x358(a1 + 3);
(v11->CryptSetKeyParam)(*v9, 1, IV, 0); // IV = parameter
v12 = m_ret_argloffset0x358(a1 + 3);
(v12->CryptSetKeyParam)(*v9, 4, 0x0001, 0); // OP_MODE = CBC
return v4;
}

```

[Update on Attacks by Threat Group APT-C-60](#)

```

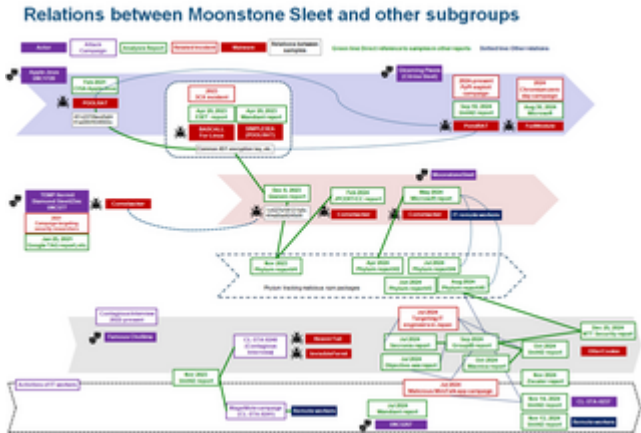
python parse_cross2beacon_config.py beacon.bin
[+] Decoded Config Data
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Encode to ASCII
000000 29 01 00 00 7f 00 00 01 b3 15 00 00 09 00 00 00 ).....
000010 31 32 37 2e 30 2e 30 2e 31 00 00 00 00 0c 01 00 127.0.0.1.....
000020 00 2d 2d 2d 2d 2d 42 45 47 49 4e 20 50 55 42 4c .----BEGIN.PUBL
000030 49 43 20 4b 45 59 2d 2d 2d 2d 2d 0a 4d 49 47 66 IC.KEY----.MIGF
000040 4d 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 MA8GCSqGS1b3DQEB
000050 41 51 55 41 41 34 47 4e 41 44 43 42 69 51 4b 42 AQUAAAGNADCB1QKB
000060 67 51 43 4e 53 33 38 6c 48 50 32 56 33 4a 44 34 gQCNS381HP2V3JD4
000070 47 54 39 55 63 61 4c 68 41 6b 70 4d 64 51 41 47 GT9UcaLhAkpM4QAG
000080 52 6e 36 4e 77 36 52 48 6e 56 35 54 2f 69 48 4a Rn6Nw6RHnVST/1H3
000090 2b 7a 48 4c 48 38 32 71 37 58 4b 6d 6f 2b 72 55 +zHLH82q7XKmo+U
0000A0 2b 49 7a 59 70 58 6e 57 55 37 70 4d 73 69 53 64 +IzYpXnwU7pMs1Sd
0000B0 71 2b 63 52 78 4d 6f 54 4c 6d 68 4e 6f 71 32 55 q+cRxoTLmhNoq2U
0000C0 54 57 4b 39 6f 39 52 6f 64 63 5a 74 5a 58 73 6b TWK9o9RodcZtZxsk
0000D0 62 4d 37 54 7a 4b 37 55 5a 6a 79 61 70 54 49 4a bM7Tzk7UZjyapTI3
0000E0 66 63 71 36 42 57 4d 64 73 4d 78 36 67 48 34 4f fcq6BwMdsMx6gh40
0000F0 73 6c 42 2f 35 77 6e 63 33 77 51 78 55 62 4f 61 s1B/Swnc3wQxUboA
000100 71 45 6f 6b 4b 6f 72 5a 77 6d 68 55 33 77 49 44 qEokKorZwmhU3wID
000110 41 51 41 42 0a 2d 2d 2d 2d 2d 45 4e 44 20 50 55 AQAB.----END.PU
000120 42 4c 49 43 20 4b 45 59 2d 2d 2d 2d 2d 41 41 41 BLIC.KEY----AAA
000130 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 .....
[+] Config Data
C2: 127.0.0.1:5555
PUBLICKEY: ----BEGIN PUBLIC KEY----
MIGFMA8GCSqGS1b3DQEBQUAAAGNADCB1QKBgQCNS381HP2V3JD4GT9UcaLhAkpM4QAGRn6Nw6
RHnVST/1H3+zHLH82q7XKmo+U+IzYpXnwU7pMs1Sdq+cRxoTLmhNoq2UTWk9o9RodcZtZxsk
bM7Tzk7UZjyapTI3fcq6BwMdsMx6gh40s1B/Swnc3wQxUboAqEokKorZwmhU3wIDAQAB
-----END PUBLIC KEY-----

```

[CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks](#)

```
movsx eax, cs:num7
movd xmm1, eax
cvtq2pd xmm1, xmm1
movsx eax, cs:num3
movd xmm0, eax
cvtq2pd xmm0, xmm0
addsd xmm0, xmm0
subsd xmm1, xmm0
mulsd xmm1, xmm1
movsd [rbp+1410+phPrev], xmm1
call ret2
movsx r9d, al
call ret0
movsx ecx, al
imul r9d, ecx
call ret7
movsx eax, al
add eax, r9d
movsx ecx, cs:num9
add eax, ecx
movsx ecx, cs:num8
xor edx, ebx
div ecx
movsx ecx, cs:num1
cmp eax, ecx
jz short loc_7FF8581895C0
call ret3
movsx edx, al
movsx eax, cs:num0
imul edx, eax
lea r9d, [edx*2]
add r9d, r9d
call ret9
movsx ecx, al
sub r9d, ecx
call ret6
movsx ecx, al
add r9d, ecx
movsx ecx, cs:num3
add ecx, r9d
```

[Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities](#)



[Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup](#)

Source: <https://blogs.jpCERT.or.jp/en/2021/02/emotet-notice.html>