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

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.

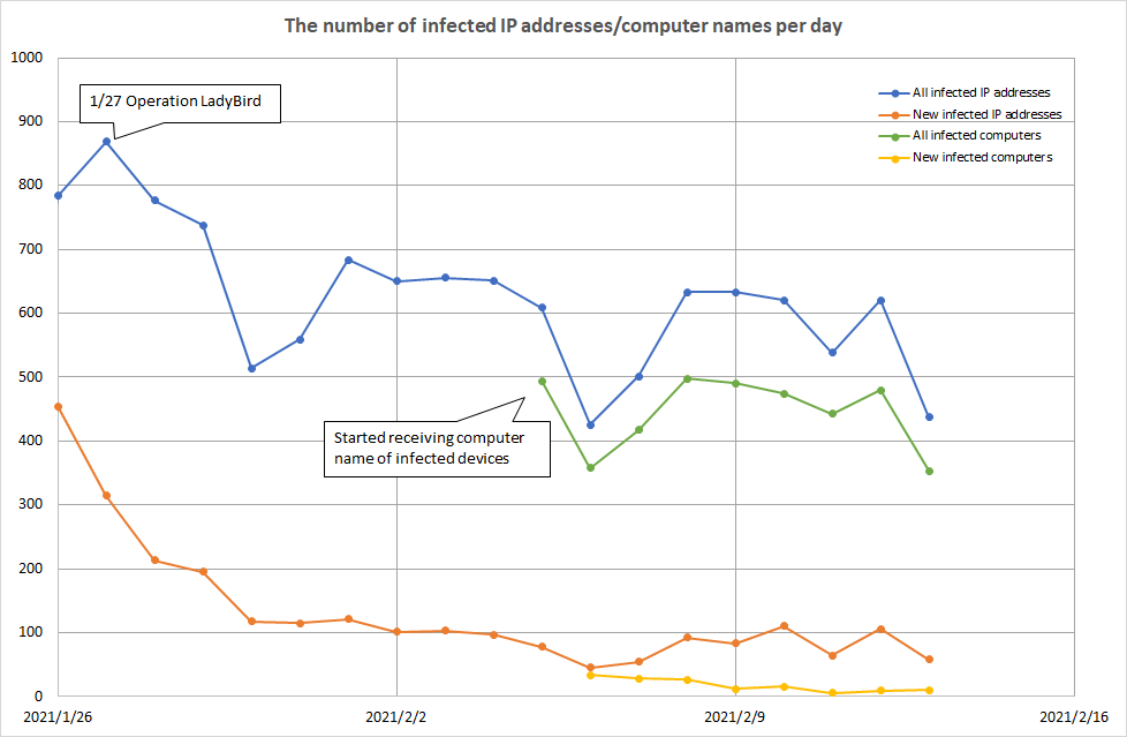


Figure 1： Emotet Infected devices in Japan

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.

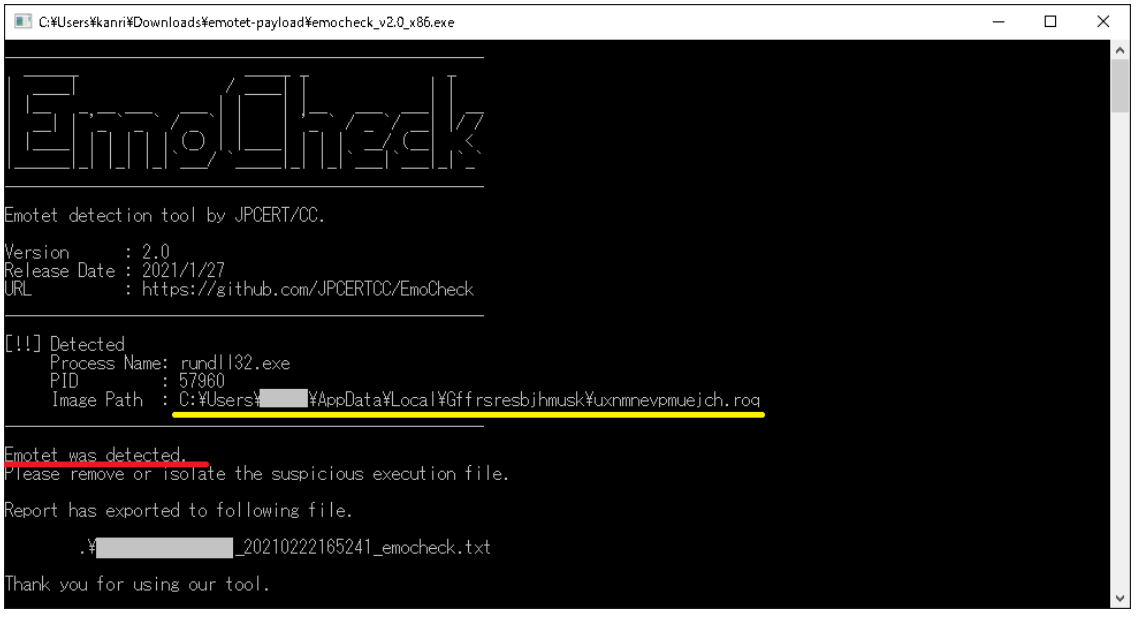


Figure 2：Sample results (Emotet detected)

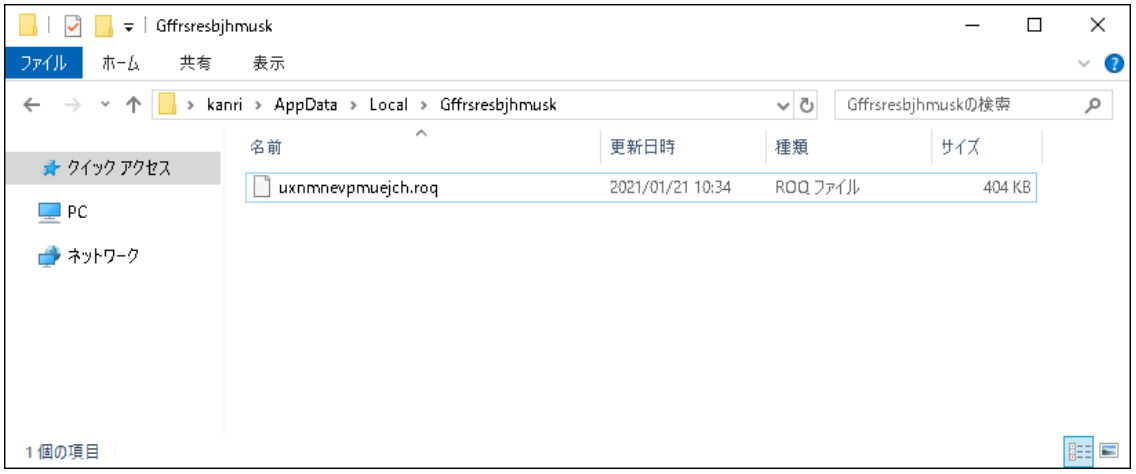


Figure 3：Sample image path of Emotet according to EmoCheck result (highlighted in yellow in Figure 2)

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.

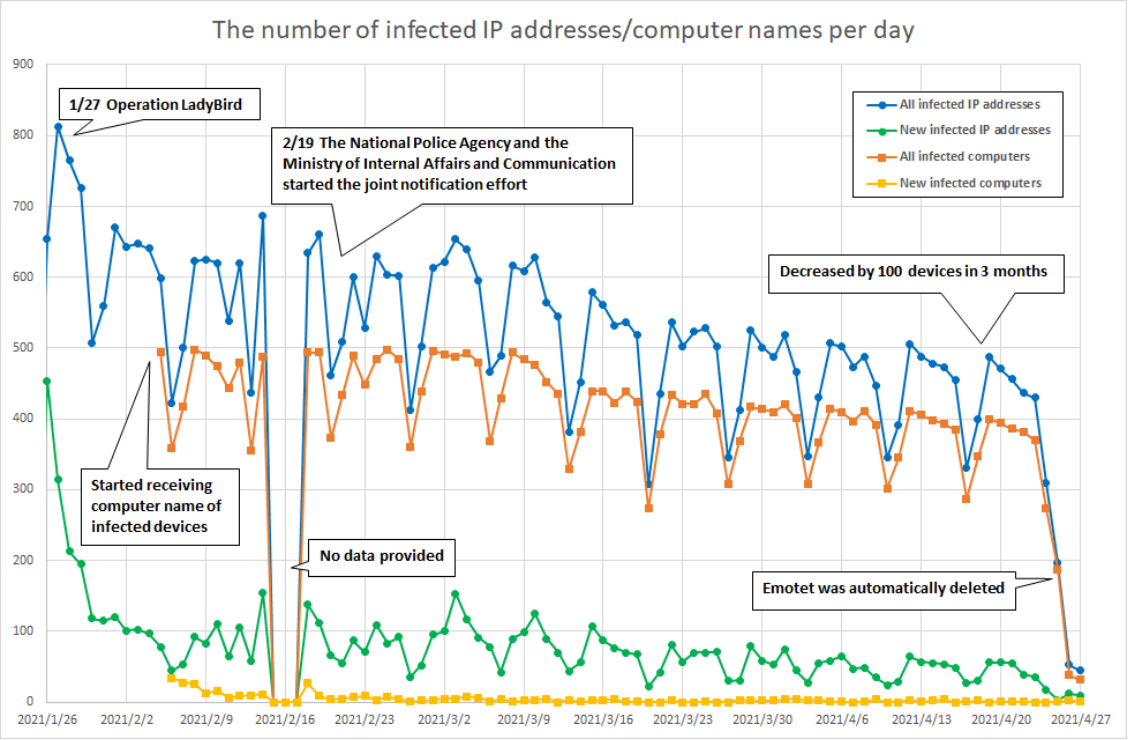


Figure 4：Emotet Infected devices in Japan

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)

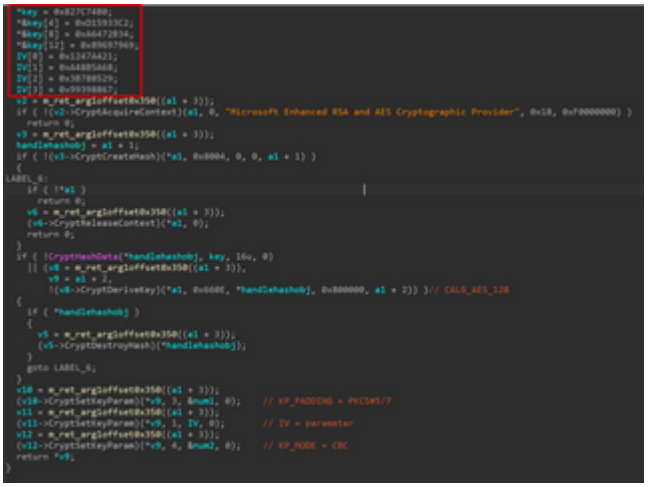
佐條 研(Ken Sajo)

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.

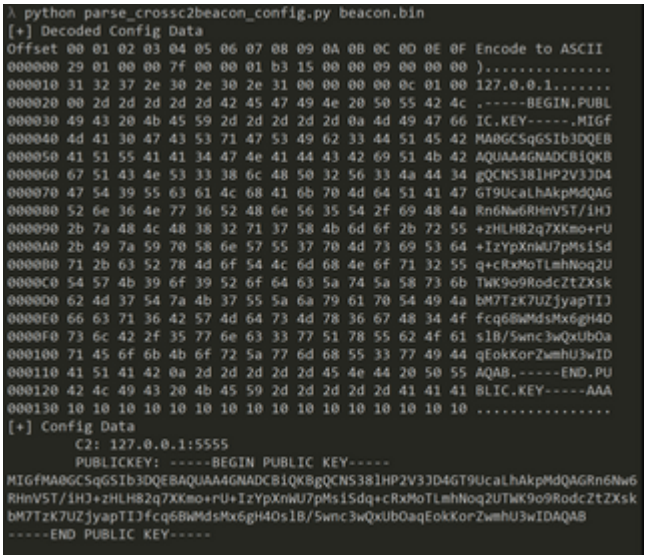
Related articles

- 

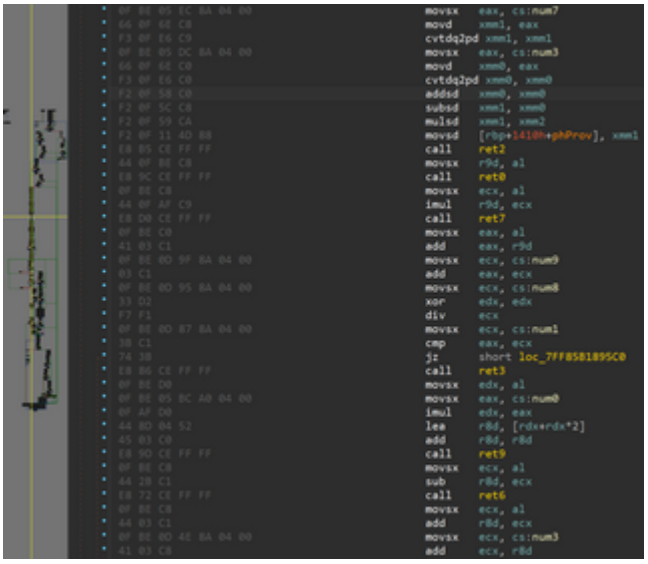
  [Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise]

- 

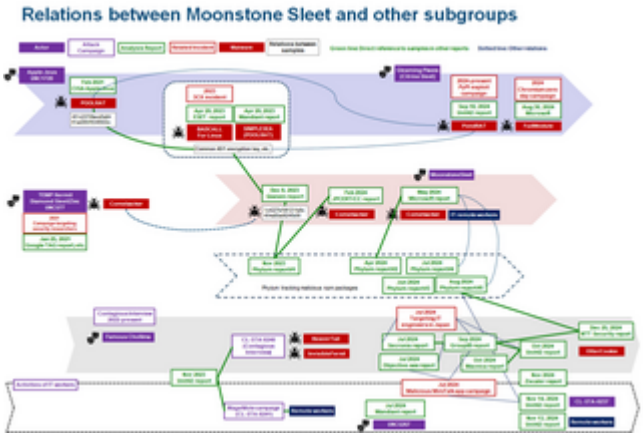
  [Update on Attacks by Threat Group APT-C-60]

- 

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

- 

  [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