More Flagpro, More Problems

cyberandramen.net/2021/12/12/more-flagpro-more-problems/

December 12, 2021

No stranger to this blog, BlackTech has continued to modify techniques to compromise networks and even suffered an OPSEC slip in the way of an open directory.

This post will cover a malicious document similar to that identified by [1] PWC and [2] NTT in the previous reporting on the group. While I cannot definitively answer that the malicious executable recovered in this case is Flagpro, I would like to highlight some of the similarities and differences found in this sample.

An Empty Excel Doc

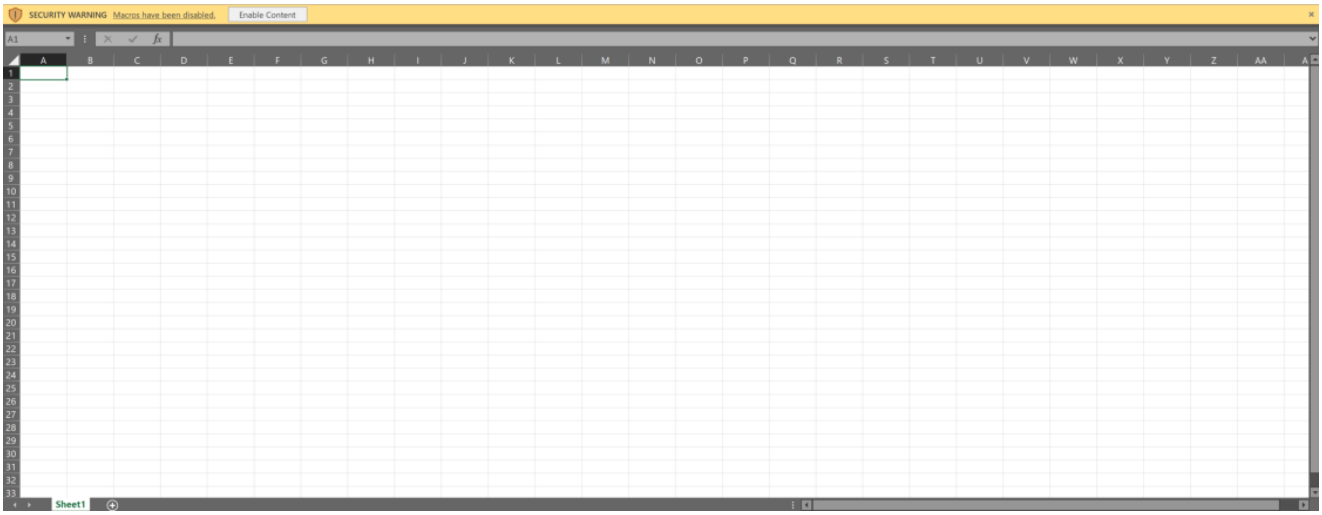

Figure 1
SHA256:0911e5d1ec48430ff9a863f5c4a38f0c71872d8bd6c89f07d6ae16d78eca162f

Filename: 2021-10工资中公积金问题咨询.xlsm (roughly translates to “Constitution on Provident Fund Issues in 2021-10 Salary”. Google Translate)

While there isn’t much in the way of a lure to entice the user to open the document, the title and delivery method would likely pique a user’s interest. Upon enabling content, a Windows executable named dwm.exe is dropped into the Startup folder which ensures persistence and is executed.

The malicious macros embedded in the Excel document are almost an exact copy of the code seen in the PWC report. Although the malicious executable is named dwm.exe, this isn’t the original name of the application as can be seen in Figure 2.

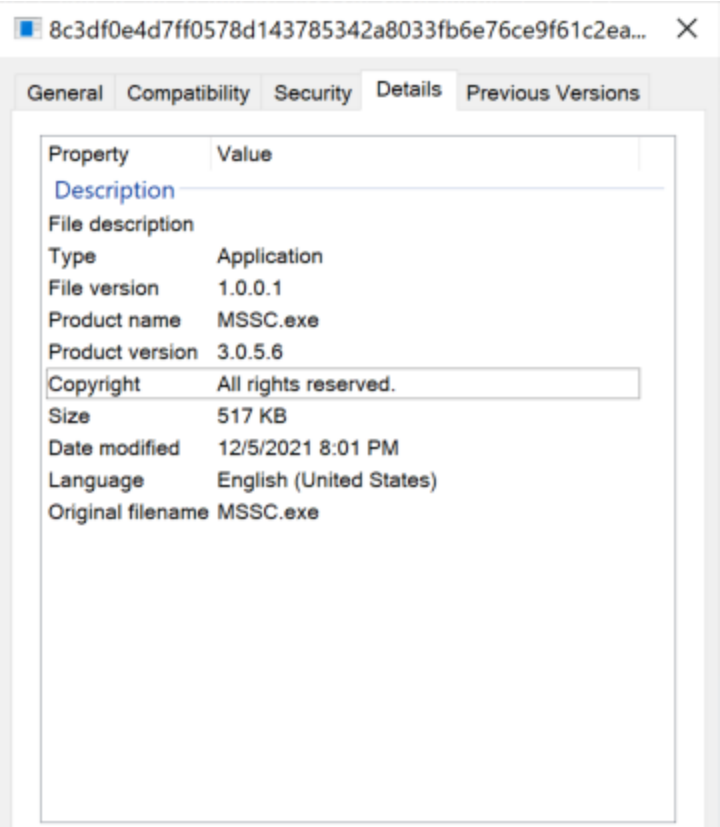

Figure 2

What's New

The Microsoft Foundation Class, or MFC is also heavily utilized in the dropped file. A number of the MFC libraries found running strings on this sample differed from previous reports on Flagpro.

Note the absence of the "CV20" prefixes in Figure 3 on the MFC classes, as reported by NTT Security. Previous reporting theorized that the CV20 served as the version number for Flagpro. This minor development change could have been in response to public reporting, or to different development practices.

```
.?AVCOleFrameHook@@
.?AVXOleInPlaceFrame@COleFrameHook@@
.?AUIOleInPlaceFrame@@
.?AUIOleInPlaceUIWindow@@
.?AVCMenu@@
.?AVXOleDocumentSite@COleDocObjectItem@@
.?AUIOleDocumentSite@@
.?AVCFile@@
.?AV?$CArray@W4LoadArrayObjType@CArchive@@AEBW412@@@
.?AV?$CTypedPtrArray@VCObArray@@PEAVCBitmap@@@@
.?AVCObArray@@
.?AVCGdiObject@@
.?AV?$CArray@PEAUHWND__@@PEAU1@@@
.?AV?$CList@PEAUHWND__@@PEAU1@@@
.?AVCFont@@
.?AVCBitmap@@
.PEAVCMemoryException@@
.?AVXAccessible@CWnd@@
.?AVXAccessibleServer@CWnd@@
.?AVCTestCmdUI@@
.?AV_AFX_HTMLHELP_STATE@@
.?AVCNoTrackObject@@
.PEAVCUserException@@
.?AV?$IAccessibleProxyImpl@VCAccessibleProxy@ATL@@@ATL@@
.?AUIAccessible@@
.?AUIDispatch@@
.?AUIAccessibleProxy@@
.?AV?$CMFCComObject@VCAccessibleProxy@ATL@@@@
.?AVCAccessibleProxy@ATL@@
.?AV?$CComObjectRootEx@VCComSingleThreadModel@ATL@@@ATL@@
.?AVCComObjectRootBase@ATL@@
.?AV_AFX_THREAD_STATE@@
```

Figure 3

In PWC's VB 2021 localhost presentation, the mutex identified for Flagpro malware began with "71564__". Mutexes associated with this sample are below.

- ZonesCacheCounterMutex
- ZonesLockedCacheCounterMutex.

Mutant	\Sessions\1\BaseNamedObjects\SM0:11488:304:WilStaging_02	0x40c
Mutant	\Sessions\1\BaseNamedObjects\SM0:11488:120:WilError_03	0x418
Mutant	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex	0x450
Mutant	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex	0x454

Figure 4

While this is certainly not a smoking gun, these are somewhat interesting development changes to the malware.

Opening the executable in Ghidra, the command and control (C2) domain is broken up over three different variables, initialized in reverse order.

Additionally, the HTTP request headers and User-Agent were similarly hardcoded and pieced back together before making a request.

```
54    undefined2 local_9b;
55    undefined local_99;
56    char local_98 [128];
57    ulonglong local_18;
58
59    local_18 = DAT_14006c970 ^ (ulonglong)auStackY1544;
60    local_188 = (HANDLE)0x0;
61    local_180 = 0;
62    local_178 = 0;
63    local_170 = 0;
64    local_438[0] = 0;
65    local_434 = 0;
66    memset(local_2ac,0,0x114);
67                        /* In text: o.sotnec (centos.o) */
68    local_b8 = 0x6f2e736f746e6563;
69                        /* In text: ifiwehtn (nthewifi) */
70    local_b0 = 0x696669776568746e;
71                        /* In text: moc. (.com) */
72    local_a8 = 0x6d6f632e;
```

Figure 5

```
if (*(longlong *)(param_1 + 0x248) != 0) {
                    /* Following vars init HTTP headers reversed */
  CONTENT-_uStack410728 = 0x2d746e65746e6f43;
  TYPE:AP_uStack410720 = 0x7061203a65707954;
  (AP)PLICATIO_uStack410712 = 0x6f69746163696c70;
  (N)\OCTET-__uStack410704 = 0x2d746574636f2f6e;
  STREAM_uStack410696 = 0xa0d6d6165727473;
  uStack410688 = 0;
  COMB_HTTP_HDRS_iVar3 = HttpAddRequestHeadersA();
  if (COMB_HTTP_HDRS_iVar3 == 0) {
    uVar8 = 0x20;
    HTTP_REQ_ERR_pcVar6 = "WinHttpAddRequestHeaders Error.\n";
```

Figure 6

Utilizing MFC classes allows threat actors to wrap Windows APIs routinely linked to malware inside the MFC library. A majority of the suspicious code can be found in the DoModal function, which houses a number of calls linked to taking screenshots of the victim's computer.

Figure 7

Network Indicators

As identified in Figure 6, dwm.exe contacted the following domain:

- centos.onthewifi[.]com
- Registrar: TLDS L.L.C. d/b/a SRSPlus
- Resolving IP: 103.195.150[.]181
- Location: Hong Kong
- Organization: Cloudie Limited

If you have read prior reporting on BlackTech intrusion operations, the above domain naming scheme should come as no surprise. Like other threat actors, BlackTech tends to use software and security companies for their C2 domain naming. The threat actor has used some form of “centos” as a C2 domain on at least four different occasions.

According to PassiveDNS (pDNS) information, centos.onthewifi[.]com previously resolved to 172.104.109[.]217. Utilizing ZoomEye to investigate the previous IP, the same “Hello Boy” C2 response NTT-Security reported on is displayed. An additional response of “1” was also found at the same IP on port 80/https.

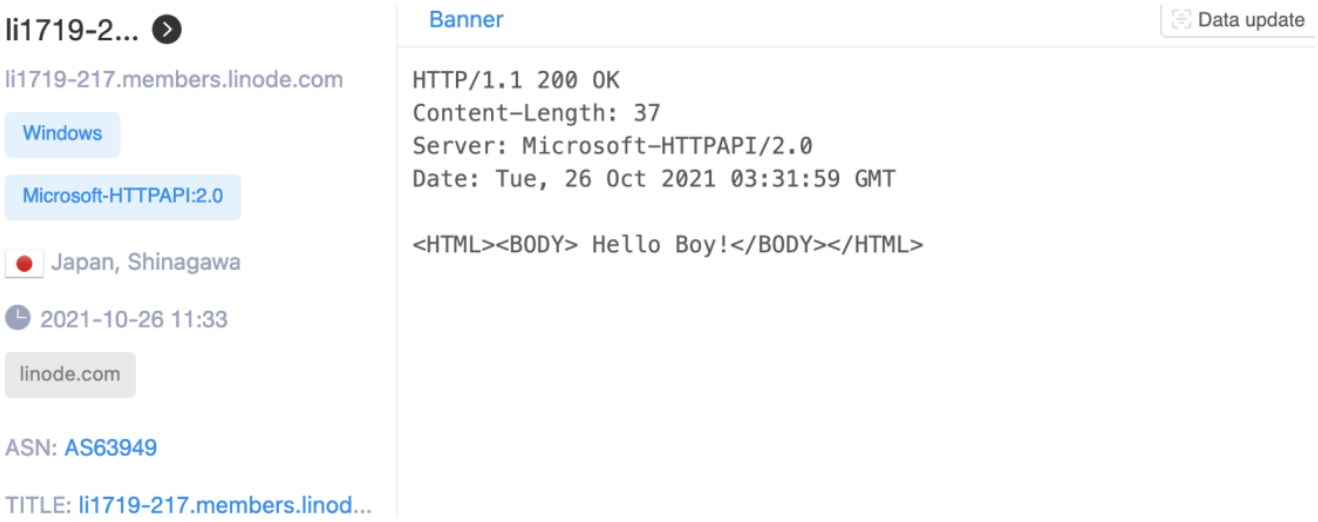

Figure 8

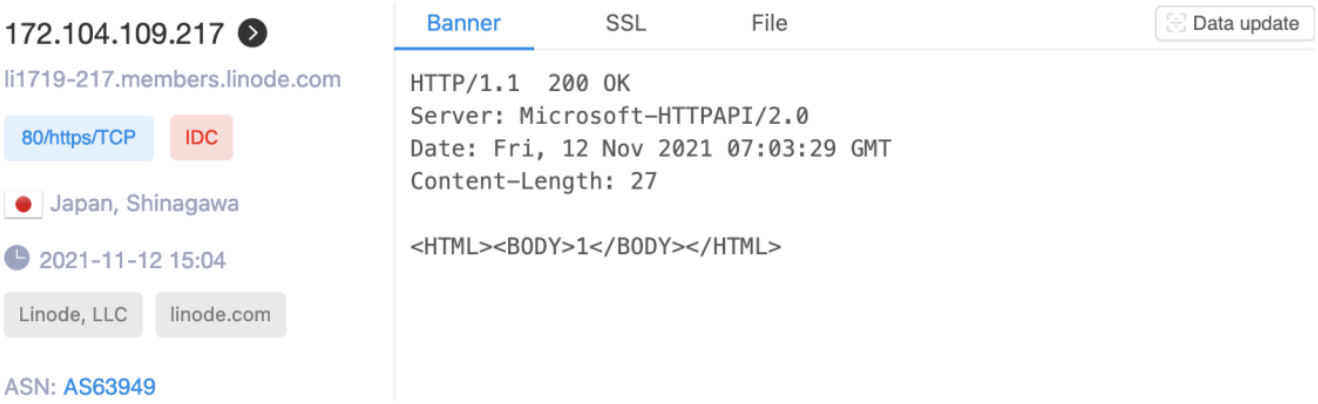

Figure 9

An additional domain possibly linked to the above is redhatstate.hopto[.]org which is also hosted at 103.195.150[.]181.

A special thanks to Twitter user, @500mk500 for noticing the above domain that matches previous BlackTech domain naming.

Conclusion

The above are not definitive links to BlackTech, however, I believe the similarities are strong enough to warrant attention and maybe a closer look by analysts. Changes in domain hosting should also be of interest to APT network infrastructure hunters, as this could be a change in technique or simply a new team has taken over procurement of network infrastructure. In any case, BlackTech remains an aggressive actor intent on cyber espionage in the APAC region.

Endnotes

[1] https://vblocalhost.com/uploads/VB2021-50.pdf

[2] https://insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro (Japanese)