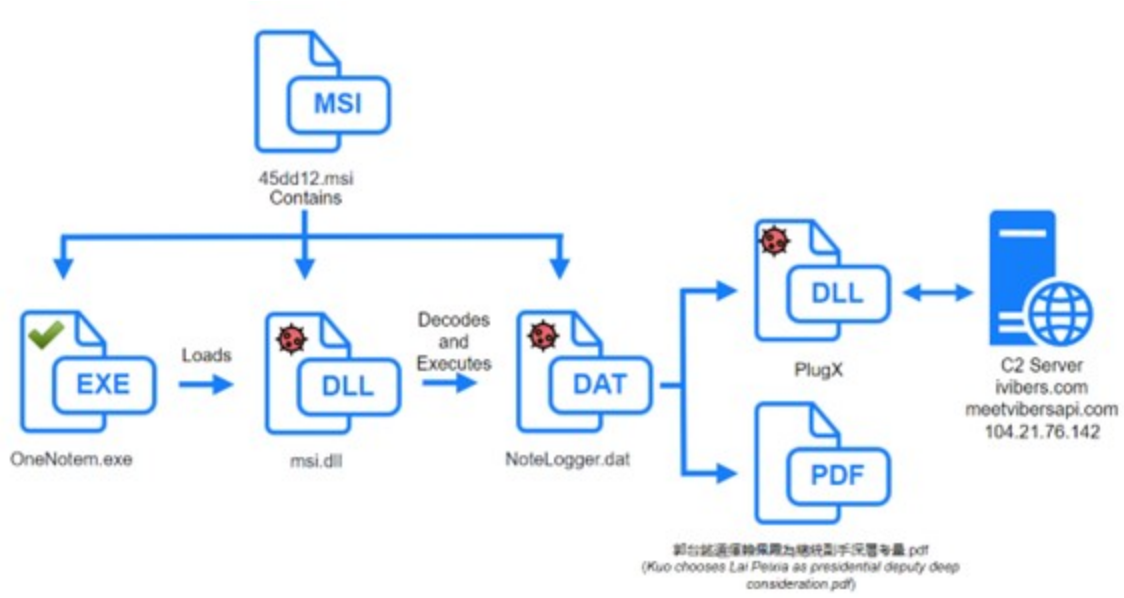
Mustang Panda's PlugX new variant targetting Taiwanese government and diplomats

lab52.io/blog/mustang-pandas-plugx-new-variant-targetting-taiwanese-government-and-diplomats/

The Lab52 team has analysed a cyber campaign in which attackers deploy a **new variant** of the **PlugX** malware. Both the infection chain and the various artefacts used in the cyberattack share **multiple similarities** with the **SmugX** campaign, attributed to threat actors **Red Delta** and **Mustang Panda**, allegedly linked to the Chinese government.

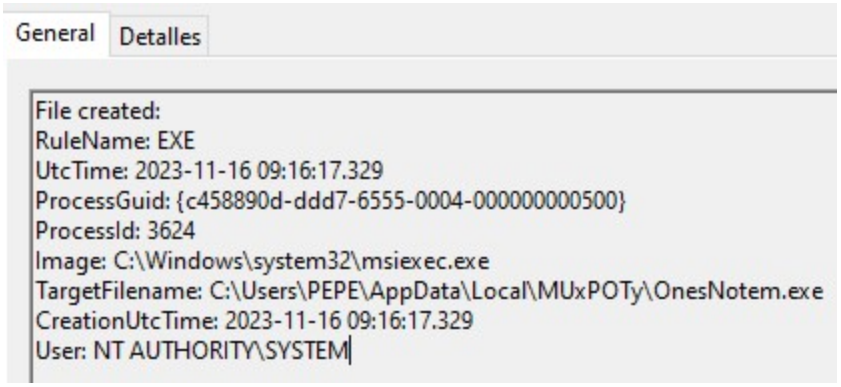
This time, the actors deploy an MSI file on victim machines containing a legitimate executable (**OneNotem.exe**), a malicious DLL (**msi.dll**) and a DAT file (**NoteLogger.dat**). The legitimate executable loads via DLL side-loading the malicious DLL and the malicious DLL decrypts and loads the DAT file into memory, which is the PlugX malware. However, this new campaign shows variations compared to previous campaigns. The **main differences** are:

- The malicious **DLL** is **written in the Nim** programming language.
- This new variant uses its **own implementation of the RC4 algorithm** to decrypt PlugX, unlike previous versions that use the Windows Cryptsp.dll library.



Killchain

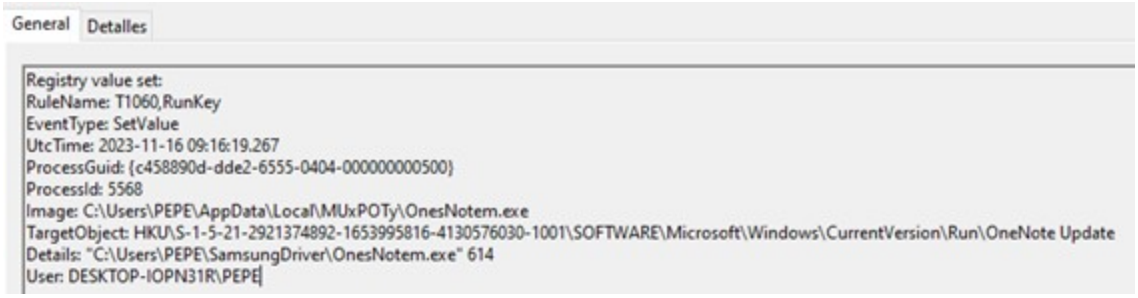
The installer file **45dd12.msi** contains the files **msi.dll**, **NoteLogger.dat** and **OneNotem.exe** and, on user execution, it copies them to the directory "**C:\UsersersuserAppData**".



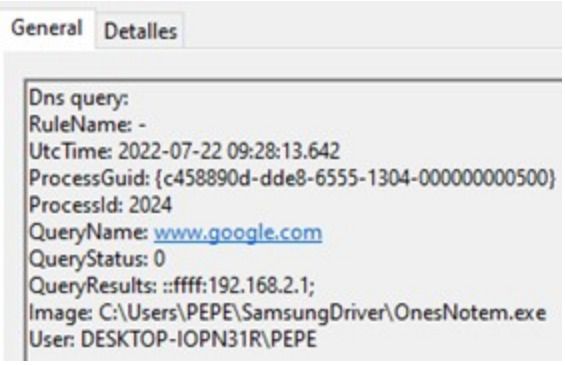
Right after, the MSI file copies OneNotem.exe to one of the following folders:

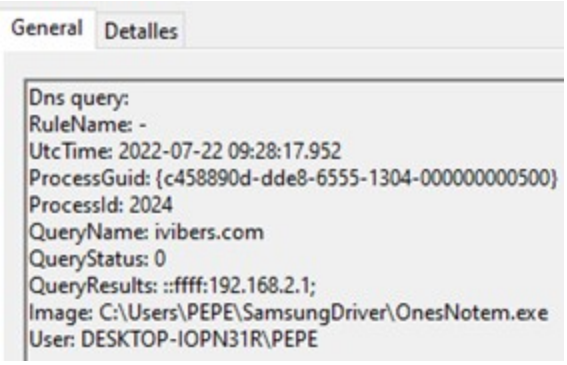
- **C:\Users\<username>\VirtualFile**
- **C:\Users\Public\VirtualFile**
- **C:\Users\<username>\SamsungDriver**
- **C:\Users\Public\SamsungDriver**
- **C:\Users\Public\SecurityScan**

In order to obtain persistence on the infected machine, the registry key "**HKEY_LOCAL_MACHINE/ SOFTWARE/ SOFTWARE/ Microsoft/ Windows/ CurrentVersion/ RunOneNote Update**" is added, which executes the legitimate **OnesNotem.exe** binary followed by a numeric parameter.



The malware then creates the process **OneNotem.exe** that will first contact with *www.google.com* to check if the computer has internet connection and then contacts the **C2 domains** *ivibers[.]com* and *meetvibersapi[.]com*. The **OneNotem.exe** process also creates a mutex to prevent the execution of a second instance.





Moving forward, Lab52's team has analysed each of the various artefacts contained in the MSI file to discern their specific roles or purposes.

MSI.DLL

This DLL contains two malicious functions, the **NimMain** function and the **MsiProvideQualifiedComponentW** function.

Name	Address	Ordinal
DllMain(x,x,x)	**6DB07BE8**	**1**
MsiProvideQualifiedComponentW	**6DB07B30**	**2**
NimMain	6DB07BC4	3
TlsCallback_0	6DB07CB4	
TlsCallback_1	6DB07D4B	
DllEntryPoint	**6DB0121C**	**[main entry]**

The **DllMain** function has been modified to add the call to **NimMain** which will be executed when the library is loaded by the **OneNotem.exe** process.

```
1 BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
2 {
3   NimMain();
4   return sub_6DB06E90(1u);
5 }
```

This will load the functions necessary for the execution of the malware. This technique is used to reduce the number of exported functions to make the analysis and possible detection of the malicious library more difficult.

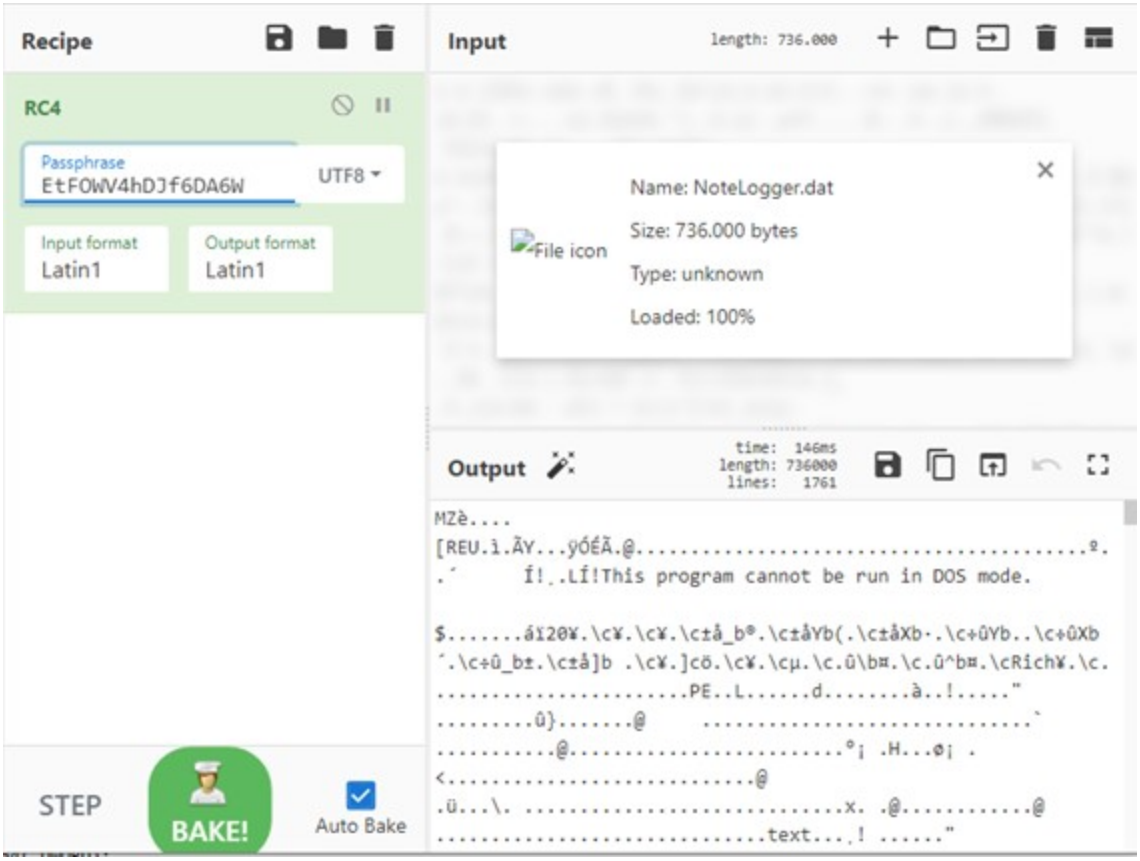
```
1  FARPROC sub_6DB0628F()
2  {
3    FARPROC result; // eax
4
5    hModule = (HMODULE)sub_6DB04B32(&unk_6DB10714);
6    if ( !hModule )
7      sub_6DB04B4B("\b");
8    dword_6DB1EA38 = (int)sub_6DB04C1A(hModule, "GetModuleFileNameW");
9    dword_6DB1EA34 = (int)sub_6DB04C1A(hModule, "GetFileAttributesW");
10   dword_6DB1EA30 = (int)sub_6DB04C1A(hModule, "FindFirstFileW");
11   dword_6DB1EA2C = (int)sub_6DB04C1A(hModule, "FormatMessageW");
12   dword_6DB1EA28 = (int)sub_6DB04C1A(hModule, "LocalFree");
13   dword_6DB1EA24 = (int)sub_6DB04C1A(hModule, "GetLastError");
14   result = sub_6DB04C1A(hModule, "FindClose");
15   dword_6DB1EA20 = (int)result;
16   return result;
17 }
```

When the legitimate executable calls the **MsiProvideQualifiedComponentW** function it will load the **NoteLogger.dat** file with the **CreateFileW** function.

```
9    if ( (_BYTE)result )
10   {
11     v1 = sub_6DB06FC4(v2);
12     result = CreateFileW(v1, 0x80000000, 3, 0, 3, 0, 0);
13     if ( result )
14       result = sub_6DB078AC(v2, result);
15   }
16   return result;
```

The malware will then copy the contents to a memory section and use the **RC4** algorithm and the key **EtFOWV4hDJf6DA6W** to decrypt a DLL contained in the **NoteLogger.dat** file, which is a **PlugX malware variant**.

```
28   v2 = sub_6DB0596D(47);
29   v24 = sub_6DB06DE6(v2, v3);
30   if ( (unsigned __int64)(v24 + 0x80000000i64) >> 32 )
31     sub_6DB043BC(v24, HIDWORD(v24), 0x80000000, -1, 0x7FFFFFFF, 0);
32   qmemcpy(v26, "EtFOWV4hDJf6DA6W", sizeof(v26));
33   if ( (int)v24 < 0 )
34     sub_6DB043BC(v24, (int)v24 >> 31, 0, 0, 0x7FFFFFFF, 0);
35   v4 = (int *)sub_6DB04D96(v24);
36   v25 = 0;
```



Finally, the DLL will be executed at location 0x00 in the memory page where it resides using the **EnumSystemGeoID** callback.

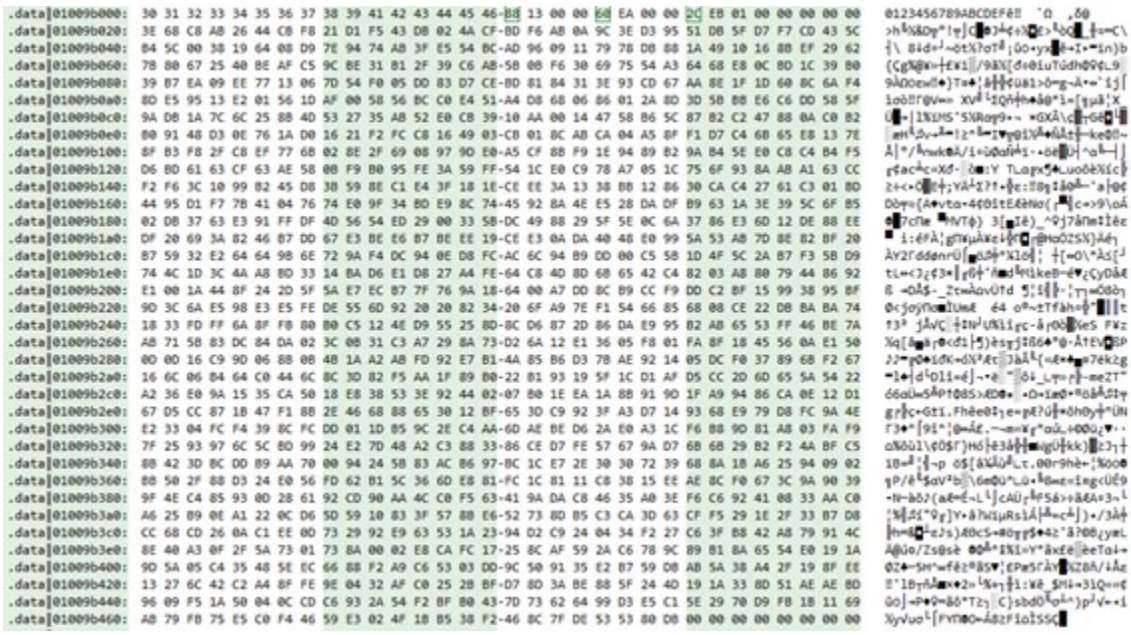
```
81    sub_6DB044EC(0, v17);
82  }
83  if ( (int)v24 < 0 )
84    sub_6DB043BC(v24, (int)v24 >> 31, 0, 0, 0x7FFFFFFF, 0);
85  qmemcpy(v23, v15 + 2, v24);
86  return EnumSystemGeoID(16, 0, v23);
87}
```

NoteLogger.dat

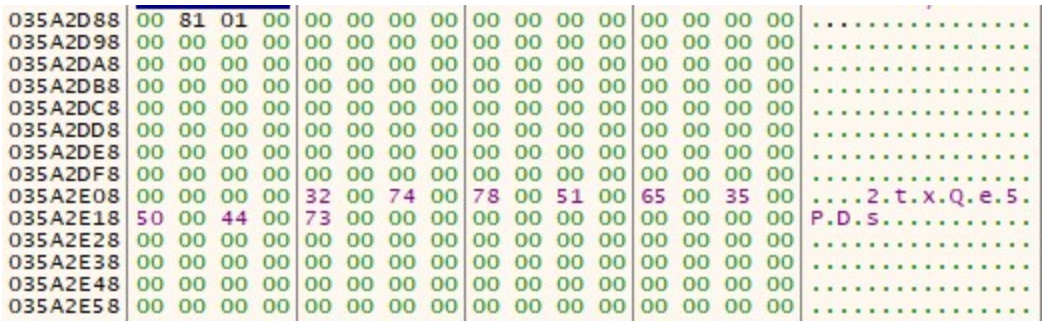
This file contains an encrypted malicious DLL, a PlugX variant, containing in **position 0x00** a small **shellcode** that will call the only function it exports. The **execution of this shellcode is indispensable** for a correct execution of the malicious DLL.

```
5FBD0000    4D              dec ebp
5FBD0001    5A              pop edx
5FBD0002    E8 00000000     call download.5FBD0007          call $0
5FBD0007    5B              pop ebx
5FBD0008    52              push edx
5FBD0009    45              inc ebp
5FBD000A    55              push ebp
5FBD000B    8BEC            mov ebp,esp
5FBD000D    81C3 59180000   add ebx,1859
5FBD0013    FFD3            call ebx
5FBD0015    C9              leave
5FBD0016    C3              ret
5FBD0017    0040 00         add byte ptr ds:[eax],al
5FBD001A    0000            add byte ptr ds:[eax],al
5FBD001C    0000            add byte ptr ds:[eax],al
5FBD001E    0000            add byte ptr ds:[eax],al
5FBD0020    0000            add byte ptr ds:[eax],al
5FBD0022    0000            add byte ptr ds:[eax],al
5FBD0024    0000            add byte ptr ds:[eax],al
5FBD0026    0000            add byte ptr ds:[eax],al
5FBD0028    0000            add byte ptr ds:[eax],al
5FBD002A    0000            add byte ptr ds:[eax],al
5FBD002C    0000            add byte ptr ds:[eax],al
5FBD002E    0000            add byte ptr ds:[eax],al
5FBD0030    0000            add byte ptr ds:[eax],al
5FBD0032    0000            add byte ptr ds:[eax],al
5FBD0034    0000            add byte ptr ds:[eax],al
5FBD0036    0000            add byte ptr ds:[eax],al
5FBD0038    0000            add byte ptr ds:[eax],al
5FBD003A    0000            add byte ptr ds:[eax],al
5FBD003C    0801            or byte ptr ds:[ecx],al         ecx:EntryPoint
5FBD003E    0000            add byte ptr ds:[eax],al
5FBD0040    0E              push cs
5FBD0041    1F              pop ds
5FBD0042    BA 0E000B409    mov edx,9B4000E
5FBD0047    CD 21           int 21
```

The malware will decrypt the configuration using the **RC4** algorithm, which is located in the "**.data**" section, similar to other samples from the SmugX campaign.



The following is the decipher configuration.



```
035A2D88 00 81 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2D98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DA8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DB8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DC8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DD8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DE8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2DF8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2E08 00 00 00 00 32 00 74 00 78 00 51 00 65 00 35 00 ....2.t.x.Q.e.5.
035A2E18 50 00 44 00 73 00 00 00 00 00 00 00 00 00 00 00 P.D.s...........
035A2E28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2E38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2E48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
035A2E58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

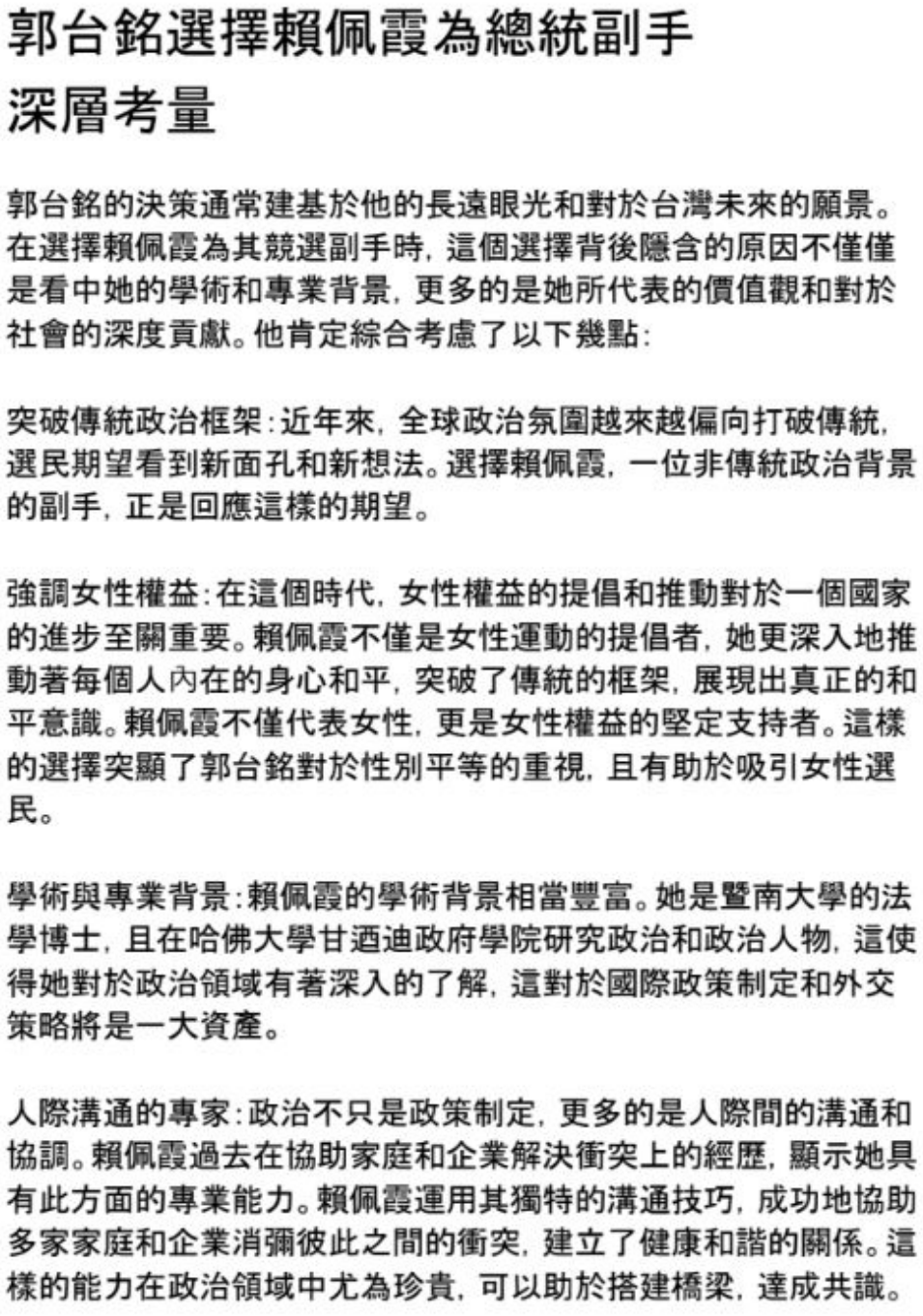

```
{
    "str_one": "",
    "str_two": " 2txQe5PD",
    "campaign_id": "tw",
    "document_name": "郭台銘選擇賴佩霞為總統副手深層考量.pdf",
    "ips": [
        {
            "ip": " ivibers.com",
                  "port": 443,
                  "is_https": 1
        },
        {
            "ip": " ivibers.com",
                  "port": 443,
                  "is_https": 1
        },
        {
            "ip": " meetvibersapi.com ",
                  "port": 443,
                  "is_https": 1
        }
    ]
```


Decoy PDF

The name and content of the lure used by the attackers seem to indicate that **the targets of this campaign are no different from those seen so far in the SmugX campaign** (diplomats and government entities). The lure uses the upcoming **Taiwanese presidential election in January 2024** to capture the interest of its victims. The document refers to Terry Gou's announcement in September this year declaring his independent candidacy for Taiwan's presidential election, with Lai Peixia as his right-hand man.

Terry Gou – who was founder and CEO of the Taiwanese multinational electronic components company -one of the largest suppliers to the United States, Europe and Japan and part of the semiconductor manufacturing cluster along with TSMC, or MediaTek- is running to bring down the current Taiwanese government, to reduce geopolitical tension and to stabilise the situation.

Lai Peixia is a singer, activist and politician with dual US-Taiwanese citizenship known for defending human rights. It seems that the attackers have used a decoy that addresses an event of high interest to political, diplomatic and governmental figures in Taiwan, as the presentation of the presidential candidacy of Terry Gou and Lai Peixia, that is particularly relevant because of the links these two political figures have with the Western bloc, the effect that their figure as president could have on Taiwan's trade relations with China, the United States, Europe and Japan and their impact on the technology race in both blocs.



郭台銘選擇賴佩霞為總統副手
深層考量

郭台銘的決策通常建基於他的長遠眼光和對於台灣未來的願景。在選擇賴佩霞為其競選副手時，這個選擇背後隱含的原因不僅僅是看中她的學術和專業背景，更多的是她所代表的價值觀和對於社會的深度貢獻。他肯定綜合考慮了以下幾點：

突破傳統政治框架：近年來，全球政治氛圍越來越偏向打破傳統，選民期望看到新面孔和新想法。選擇賴佩霞，一位非傳統政治背景的副手，正是回應這樣的期望。

強調女性權益：在這個時代，女性權益的提倡和推動對於一個國家的進步至關重要。賴佩霞不僅是女性運動的提倡者，她更深入地推動著每個人內在的身心和平，突破了傳統的框架，展現出真正的和平意識。賴佩霞不僅代表女性，更是女性權益的堅定支持者。這樣的選擇突顯了郭台銘對於性別平等的重視，且有助於吸引女性選民。

學術與專業背景：賴佩霞的學術背景相當豐富。她是暨南大學的法學博士，且在哈佛大學甘迺迪政府學院研究政治和政治人物，這使得她對於政治領域有著深入的了解，這對於國際政策制定和外交策略將是一大資產。

人際溝通的專家：政治不只是政策制定，更多的是人際間的溝通和協調。賴佩霞過去在協助家庭和企業解決衝突上的經歷，顯示她具有此方面的專業能力。賴佩霞運用其獨特的溝通技巧，成功地協助多家家庭和企業消彌彼此之間的衝突，建立了健康和諧的關係。這樣的能力在政治領域中尤為珍貴，可以助於搭建橋梁，達成共識。

Decoy PDF: Kuo's in-depth considerations for choosing Lai Peixia as presidential VP.pdf

Indicators of Compromise

c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1
651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859
908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8
c6ef220d0c6e9015bdfb7977ff15e7f2c4c0dbfcd3b28ffb3066fe6d21251322
8af3fc1f8bd13519d78ee83af43daaa8c5e2c3f184c09f5c41941e0c6f68f0f7
45dd12.msi
msi.dll
NoteLogger.dat
郭台銘選擇賴佩霞為總統副手深層考量.pdf
ivibers[.]com
meetvibersapi[.]com