Part 1: Quick analysis of malicious sample forging the official dispatch of the Central Inspection Committee - VinCSS Blog

By Yến Hứa

Published: 2021-05-12 · Archived: 2026-04-05 14:49:37 UTC

Through continuous cyber security monitoring, VinCSS has discovered a document containing malicious code with Vietnamese content that was found by ShadowChaser Group(@ShadowChasing1) group. We think, this is maybe a cyberattack campaign that was targeted in Vietnam, we have downloaded the sample file. Through a quick assessment, we discovered some interesting points about this sample, so we decided to analyze it. This is the **first part** in a series of articles analyzing this sample.

- 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

Extracting this **.docx** file and examining the extracted **.xml** files, we discovered that this **.docx** file was created and modified on Kingsoft Office software, which is a popular word processing and document creation in China.

We found **KSOProductBuildVer = 2052-11.1.0.10228**. Search by this value, we guess it could be **Kingsoft Office 2019** version.

Continue analyzing file with **olevba** tool:

With olevba's results, it can be seen that this document applies Template Injection technique.

The advantage of this technique is that when the user open the file, it will automatically download the **Main.jpg** file from the address **hxxp://45[.]121[.]146[.]88/Apricot/Main.jpg**.

Up to the time of our analysis, the Main.jpg file is still downloadable:

Main.jpg is an RTF file:

According to our analysis experience, these RTF files are often used to exploit vulnerabilities in Equation Editor. Check the file with **rtfobj**:

Based on the results in above picture , we can determine that when executing the **Main.jpg** file, it will drop the **5.t** file into the **%Temp%** directory, through exploiting the vulnerability in the Equation Editor to execute the shellcode, and then decode **5.t** and execute this file. At this point, there are two methods to decode **5.t**:

- **Method 1**: use rr_decoder.
  - Use **rtfobj** to extract **5.t**.

- Use **rr_decode.py** for decoding to get payload:

- **Method 2**: Let's the malware to perform its task by opening the RTF file, it will decrypt the **5.t** payload and create a scheduled task to execute this file:

Check the decrypted file (d198c4d82eba42cc3ae512e4a1d4ce85ed92f3e5fdff5c248acd7b32bd46dc75), this is a dll file with the original name **Download.dll**. This file has only one exported function which is **StartW**:

Through examining the **Download.dll** file, we see it was built with Visual Studio 2019, linker version 14.28. TimeDateStamp at build time is Thursday, 01.04.2021 01:59:48 UTC. This value is consistent in TimeDateStamp in FileHeader and Debug Info, type ILTCG.

RichID information identified that the version of Visual Studio 2019 that the hacker is using is 16.8. The current version of Visual Studio 2019 is 16.9(.6).

During the analysis of this Download.dll file, we discovered indicators of the same code base, reused from a previous campaign of an APT Panda group that was targeted in Vietnam. The decoy document of that campaign is Dt-CT-cua-TTg.doc. **Dt-CT-cua-TTg.doc** file is also an RTF file, which also takes advantage of Equation's bug to execute shellcode and drop the first stage payload. For more information please read here.

In the next part, we will analyze **Download.dll** file in detail, showing the similarities in the source code in this file and other PE files in the later payloads of the above campaign analysis.

Truong Quoc Ngan (aka HTC)

Tran Trung Kien (aka m4n0w4r)

Malware Analysis Expert

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