DeepCDR RTF SnakeKeyLogger Malware attack

Written by Dr. Ran Dubin

This review is written as part of DeepCDR RTF research paper.
The SnakeKeyLogger md5: 74ab9855f26b0cc2fca1fefd566f5642
From the interactive sandbox named Any.Run we can see that when running the file (winword.exe is word application) the malware used PowerShell and cmd.exe (command line) to run the next phases of the attack until it downloads mum.exe which is the snakeLoader malware.

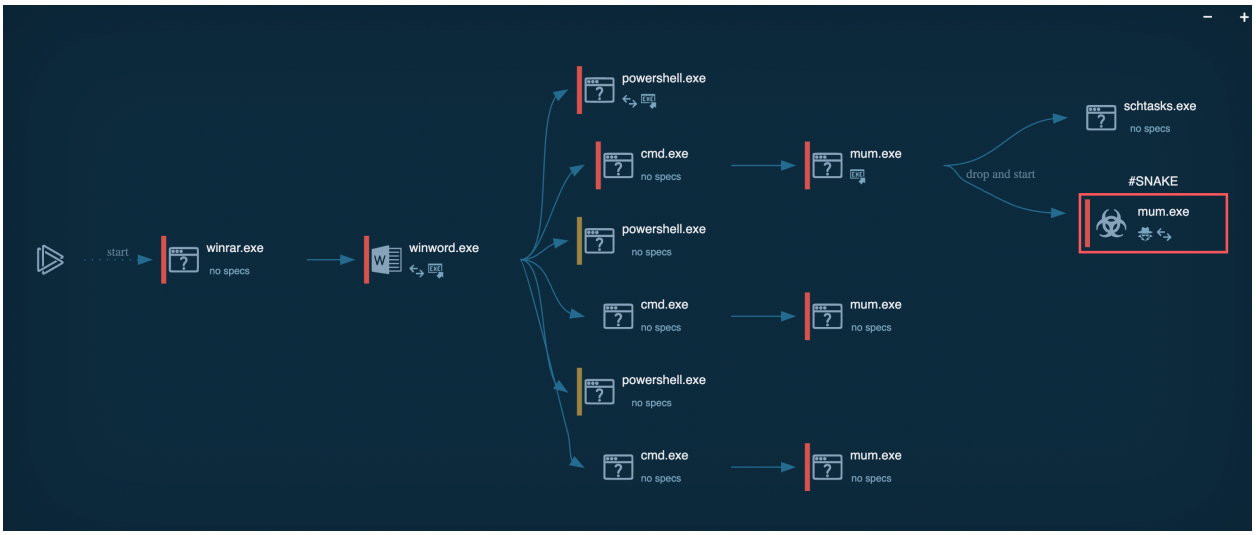


Figure 1. Any.Run sandbox analysis

Detected by VirusTotal today 19/9/22 with 35 engines out of 60.

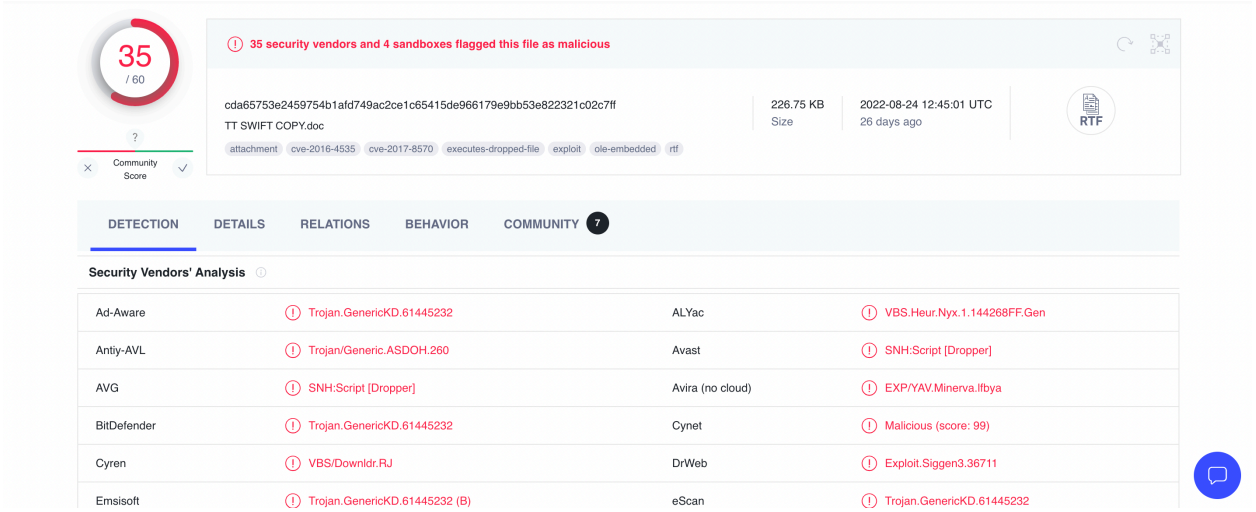


Figure 2. VirusTotal detection before CDR

Currently, 4 sandboxes detect the file as malicious in VirusTotal.

When we examine RtfObj we can see it contains known exploits and a suspicious object which is an executable file. Winword.exe is actually downloading the malicious file from a malicious website: http[:]//f0705964[.]xsph[.]ru/mum[.]exe

```
---+----------+------------------------------------------------------------
id |index     |OLE Object
---+----------+------------------------------------------------------------
0  |0000095Dh |format_id: 2 (Embedded)
   |          |class name: b'package'
   |          |data size: 20019
   |          |OLE Package object:
   |          |Filename: 'DRdtfhgYgeghDp\xa0.scT'
   |          |Source path: 'C:\\nsdsTggH\\DRdtfhgYgeghDp\xa0.scT'
   |          |Temp path = 'C:\\8jkepaD\x87\\DRdtfhgYgeghDp\xa0.scT'
   |          |MD5 = 'e9b62f3d61d226efe8d4a3fcf1c15d30'
   |          |EXECUTABLE FILE
   |          |File Type: Unknown file type
---+----------+------------------------------------------------------------
1  |0000ACF5h |format_id: 2 (Embedded)
   |          |class name: b'OLE2LInk'
   |          |data size: 2560
   |          |MD5 = '7cab6fbed3f65c729c34ab23627ad577'
   |          |CLSID: 00000300-0000-0000-C000-000000000046
   |          |StdOleLink (embedded OLE object - Known Related to
   |          |CVE-2017-0199, CVE-2017-8570, CVE-2017-8759 or CVE-2018-8174)
---+----------+------------------------------------------------------------
```

Figure 3. RtfObj Detection before CDR

When we examine our Yara detection we get the following signatures:
INDICATOR_RTF_Exploit_Scripting
cda65753e2459754b1afd749ac2ce1c65415de966179e9bb53e822321c02c7ff.rtf
INDICATOR_RTF_MalVer_Objects
cda65753e2459754b1afd749ac2ce1c65415de966179e9bb53e822321c02c7ff.rtf

When we run the CDR in VirusTotal:
We can see this file was upload a minute ago and the file type is RTF.
The file was not detected as malicious the original filename after CDR is still the same but the md5 is different since the file content has changed.
Now the md5 is: fa160de3813bafeb6d5f708dc7e5c940

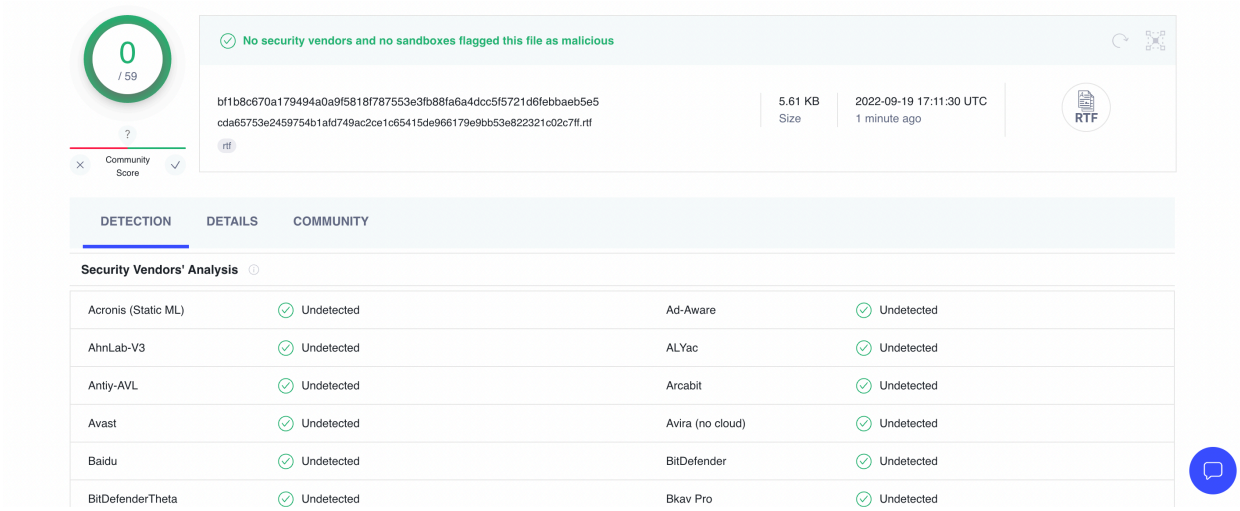


Figure 4. VirusTotal Detection after CDR

When examining the RtfObj tool now:

```
---+----------+-----------------------------------------------------------------
id |index     |OLE Object
---+----------+-----------------------------------------------------------------
```

Figure 5. RtfObj Detection After CDR

We can observe no detected malicious indicators.
When we run Yara tools: we do not detect any signature.

We can observe that the image before CDR and After CDR looks the same:

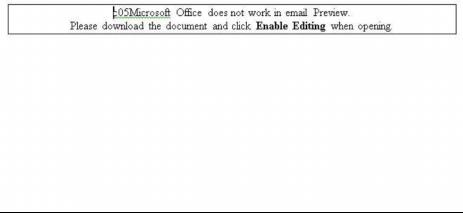
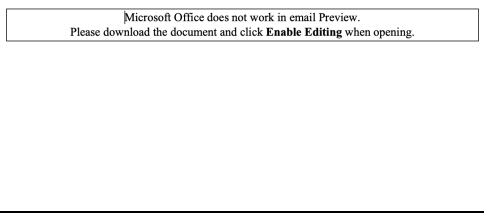
Document Preview Before CDR	Document Preview After CDR
	

Figure 6. Comparison before and after CDR

Since our algorithm replaced the fonts for enhanced security, we can see small changes here. However, the file is fully functional, and we can edit it without a problem and malware. Note that we do not have to replace the fonts, but in some cases, Fonts can be an attack vector.