Telsy

Cyber Reports

Google Drive abused in document exfiltration operation against Afghanistan

06/07/2021

INDEX

1 Introduction

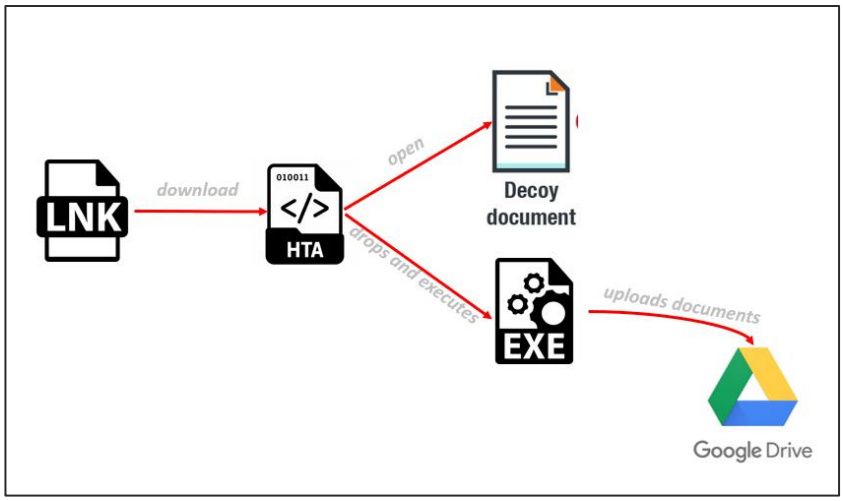
Telsy last June analyzed a new campaign that targeted Afghanistan, specifically researchers and government employees. The attack aimed to steal documents from the attacked systems and put them in an external Google Drive. Most likely, the attack was conducted via spear-phishing and also used a decoy document to hide the real actions.

The peculiarity of the attack is that the payload, which opens the decoy document and released the malware into the system, was hosted on an Indian website "hxxps://dadsasoa.in", which is linked to the Defense Accounts Department (DAD) of India. The Defense Accounts Department (DAD) operates under the administrative control of India's Ministry of Defense and is headed by the Controller General of Defense Accounts.

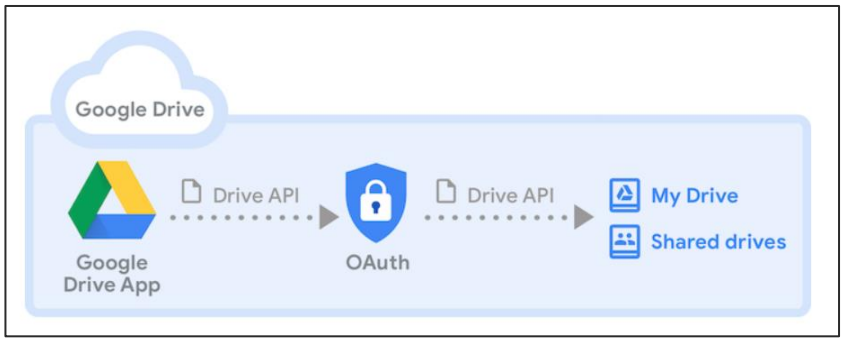
The website has been, several times, used as an infection vector due to compromise, i.e. allowing the download of malicious payloads.

2 Analysis

The attack starts with a lnk file, most likely, sent as attachment through mail. The shortcut downloads from a website “hxxps://dadsasoa.in” an **hta** file and then execute it. The **hta** is a javascript file that open a decoy document and drops the real payload to exfiltrate documents. The final payload, i.e. **winstr.exe**, is used just to exfiltrate documents of the system uploading them to a private Google Drive. Once executed, the malware will check for the following file types in certain locations to upload them into Google Drive: pdf, doc, docx, xls, xlsx, ppt, pptx and txt.



This malware is written in **GOLang** and uses the common libraries to interact with Google Drive API. In order to use the Google Drive API, it's required to create a Google application and then the account that wants to use the API should 'agree' and install the application.



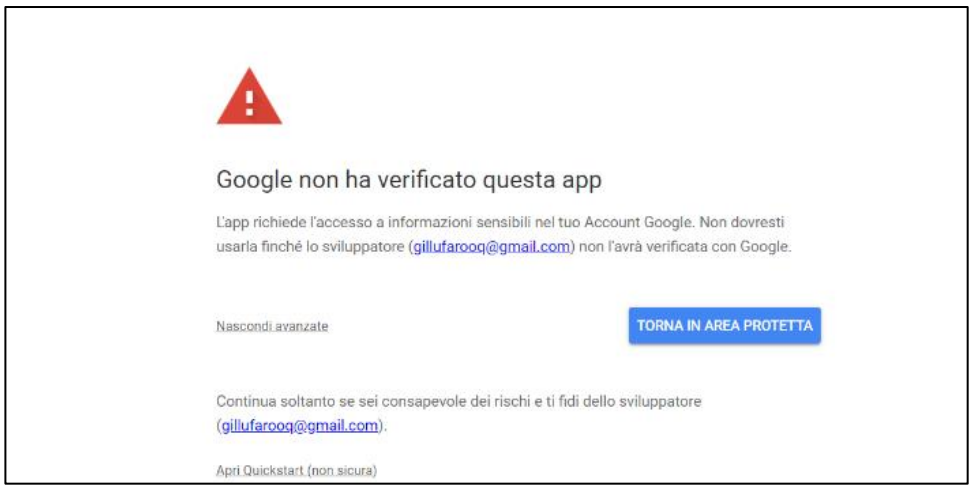
In order to upload the files to Google Drive, the client_id and client_secret were embedded on the malware, together with a refresh token. Refresh tokens are needed as part of the OAuth 2.0 protocol, which is used by Google Drive. This protocol is used by Twitter,

Facebook and other sites to use their accounts to log in to a different website. Access tokens are used to have access on a Google Drive account. However, access tokens expire so refresh tokens are needed to get new access tokens.

The credentials used to configure the Google Drive client are listed below.

Once the access token expires, the application uses the refresh token, that never expires, to obtain a new one.

If you try to install the google application, it is highlighted that the app is not signed and the developer's email revealed: gillufarooq[@]gmail.com.



Then, the research has been driven to the Google Drive, trying to figure out wich entity was compromised. Indeed using the information hardcoded in the sample, we were able to list the files on the Google Drive and get some information on the owner of the drive self.

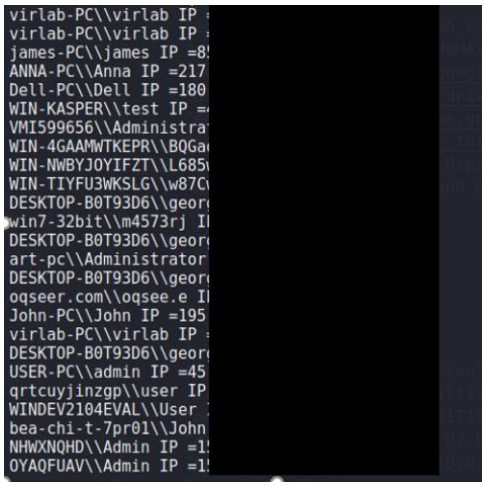

```
{
 "kind": "drive#about",
 "etag": "\"0vf5Ui-B5AgHqSXcSqpL1coKys4\"",
 "selfLink": "https://www.googleapis.com/drive/v2/about",
 "name": "Da Afghanistan Bank bank",
 "user": {
  "kind": "drive#user",
  "displayName": "Da Afghanistan Bank bank",
  "picture": {
   "url": "https://lh3.googleusercontent.com/a-/AOh14GjWxHztTjT2HCvWn44s-CCnEHrXzEZ82g5shx8l=s64"
  },
  "isAuthenticatedUser": true,
  "permissionId": "10166731120214934250",
  "emailAddress": "daafghanistanbankbank@gmail.com"
 },
 "quotaBytesTotal": "16106127360",
 "quotaBytesUsed": "1464067691",
 "quotaBytesUsedAggregate": "1464067691",
 "quotaBytesUsedInTrash": "202925485",
 "quotaType": "LIMITED",
 "quotaBytesByService": [
  {
   "serviceName": "DRIVE",
   "bytesUsed": "1464067691"
  },
  {
   "serviceName": "GMAIL",
   "bytesUsed": "0"
  },
  {
   "serviceName": "PHOTOS",
   "bytesUsed": "0"
  }
 ],
```


The Google Drive owner is: daafghanistanbankbank[@]gmail.com. The account uses the following logo as profile image:

The reverse image search confirmed that the owner of the logo is "Da Afghanistan Bank" (https://www.dab.gov.af/About-DAB-Logo)

Since the gmail space used is 0 bytes and photos space too, it is most likely that this account is not a compromised one but just an account created by the attacker. Another evidence of this, is that this email seems to be not available on official channels of the Afghanistan.

First thing done was to list the directories and through the Ips trying to discern the virtual machine and real attacked systems.



Some of these are virtual machine used to analyze malwares, some other are real victims of the campaign like:

- Dell-PC\\Dell IP =180.94.xx.xx

This IP uploaded something like 5000 documents, most of them are government communications and letters between governement employees. The system infected seems to belong to an office manager of Ministry of Borders and Tribal Affairs of the Afghanistan.

This type of spear-phishing campaign, using Google Drive as an exfiltration channel, manages to evade the main detection systems as it generates traffic that is not categorized as malicious.

Further IoCs, Yara / Sigma rules and a deeper report in PDF format are available by subscribing a Telsy Threat Intelligence service

3 Indicators of Compromise

HASH	Value	FileType
SHA1	bf080d946ab5ab93a821c345b7e7f25f22b5fbce	LNK
SHA1	1af2b3f912074a98ff9e1f6b8ecffa4cbdeedb5c	HTA
SHA1	9c9b57bf8ed287859ed6d06b988005c41219d30a	PE32 EXE
URL		
https://dadsasoa.in/font/js/images/files/United-States_Project_for_Promise/css		
EMAIL		
gillufarooq[@]gmail.com		
daafghanistanbankbank[@]gmail.com		

4 ATT&CK Matrix