January 17, 2017 | 5 min read

Carbanak Group uses Google for malware command-and-control

X-Labs

google malware

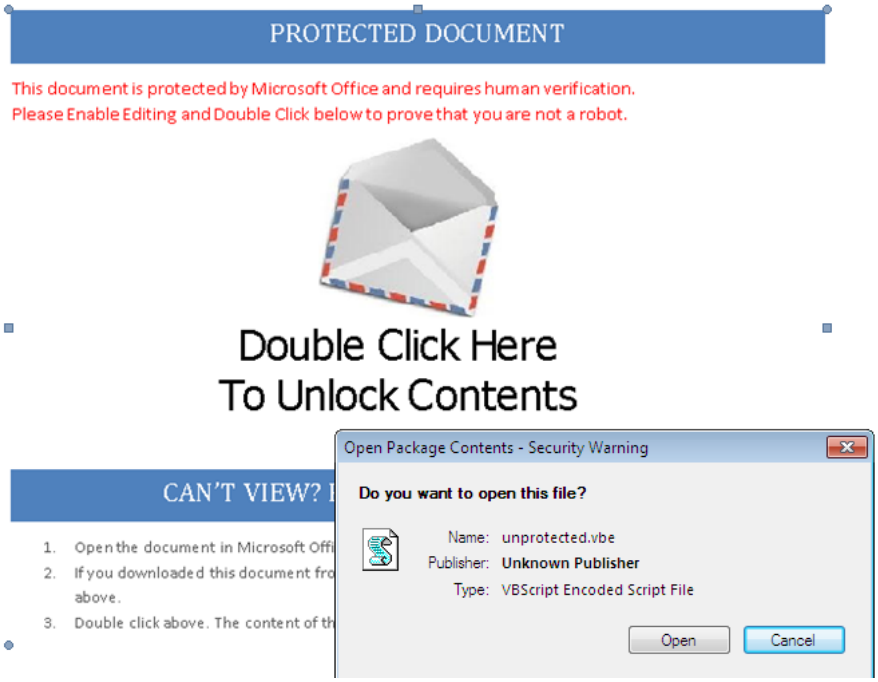
In the article

Forcepoint Security Labs™ recently investigated a trojanized RTF document which we tied to the Carbank The document contains an encoded Visual Basic Script (VBScript) typical of previous Carbanak malware samples of the malware have now included the ability to use Google services for command-and-control (C&C communication. We have notified Google of the abuse and are working with them to share additional informat

Carbanak (also known as Anunak) are a group of financially motivated criminals first exposed in 2015. The actors from financial institutions using targeted malware. Recently a new Carbanak attack campaign dubbed "Digital F exposed where the group used weaponized office documents hosted on mirrored domains, in order to distribut

Weaponized document

The RTF document we analyzed (SHA1 1ec48e5c0b88f4f850facc718bbdec9200e4bd2d) has an embedded OL contains a VBScript file. When the document is opened the targeted user is lured into double-clicking on the er object which is disguised as an image:



Double clicking on the image results in a file open dialog for "unprotected.vbe". If the user executes this file ther malware will begin to execute.

Encoded VBScript malware

The VBScript malware inside the RTF document (SHA1 cd75662751c59951717b4704ea2cdb6fb7ec19bc) is an en file. We decoded the script and found hallmarks typical of the Carbanak group's VBScript malware, however we addition of a new "ggldr" script module.

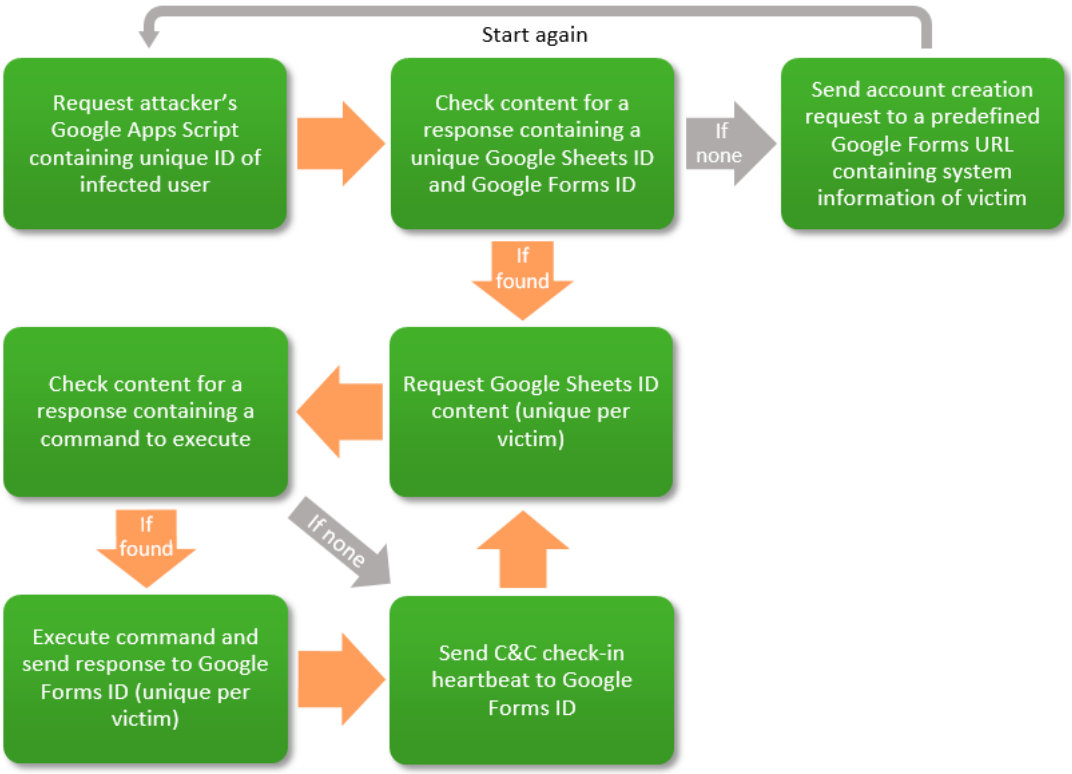
```
dIm box
box="RFFwYlRHRnpkRU50WkZObFkzUnBiMjVkRFFwc1lYTjBYMk50WkY5cFpEMHhEUW9OQ2x0U2RXNVRaV04wY...
dIm gGldr
ggldr="T24gRXJyb3IgUmVzdW1lIE5leHQNCmRpbSBleGVjRmlsZU5hbWUsIHN0YXJ0RmlsZU5hbWUNCmV4ZWN...
```

The module is base64 encoded inside the main VBScript file along with various other VBScript modules used b When we analyzed the script we noticed that it is capable of using Google services as a C&C channel.

Abusing Google for C&C communication

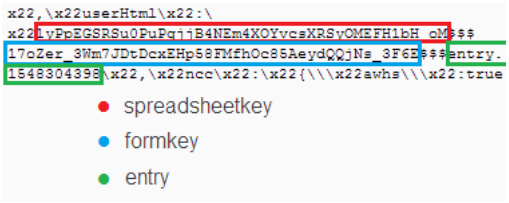
The "ggldr" script will send and receive commands to and from Google Apps Script, Google Sheets, and Google For each infected user a unique Google Sheets spreadsheet is dynamically created in order to manage each vic legitimate third party service like this one gives the attacker the ability to hide in plain sight. It is unlikely that the Google services are blocked by default in an organization, so it is more likely that the attacker will establish a C& successfully.

The C&C procedure is outlined in the diagram below.



Upon the first attempt to contact the hard-coded Google Apps Script URL with the user's unique infection ID, th that no spreadsheet currently exists for the user. The malware will then send two requests to another hard-code URL which will result in the creation of unique Google Sheets spreadsheet and Google Form IDs for the victim.

The second time the Google Apps Script is requested, the C&C will return the unique Google Sheet and Google



The "entry" value is also a unique ID which is sent with each subsequent Google Forms C&C request.

Protection statement

Forcepoint™ customers are protected against this threat via TRITON® ACE at the following stages of attack:

Stage 5 (Dropper File) - The malware components are prevented from being downloaded and/or executed.

Stage 6 (Call Home) - The HTTP-based Carbanak C&C traffic is blocked.

Summary

The Carbanak actors continue to look for stealth techniques to evade detection. Using Google as an independe is likely to be more successful than using newly created domains or domains with no reputation. Forcepoint will

monitor this group's activities and share data with trusted partners.

Indicators of Compromise

Carbanak Documents

1ec48e5c0b88f4f850facc718bbdec9200e4bd2d (3-ThompsonDan.rtf)
400f02249ba29a19ad261373e6ff3488646e95fb (order.docx)
88f9bf3d6e767f1d324632b998051f4730f011c3 (claim.rtf)

Carbanak Google Apps Script C&Cs

hxxps://script.google[.]com/macros/s/AKfycbzuykcvX7j3TlBNyQfxtB1mqii31b4VTON640yiRJT0t6rS4s4/exec
hxxps://script.google[.]com/macros/s/AKfycbxxx5DHr0F8AYhLuDjnp7kGNELq6g27J4c_JWWx1p1nDfZh6lnO/e
hxxps://script.google[.]com/macros/s/AKfycbwZHCgg5EsCiPup_mNxDbSX7k7yBMeXWenOVN1BWXHmyBpb

Carbanak Google Forms C&Cs

hxxps://docs.google[.]com/forms/d/e/1FAIpQLScx9gwNadC7Vjo11mXLbU3aBQRrqVpoWjmNJ1ZneqpjaYLE3g
hxxps://docs.google[.]com/forms/d/e/1FAIpQLSfE9kshYBFSDAfRclW8m9rAdajqoYhzhEYmEAgZexE3LQ-17A/
hxxps://docs.google[.]com/forms/d/e/1FAIpQLSdcdE7ITEiqV5MW3Up8Hgcy5NGkIKnLKoe0YPFriD4_9qYq9A/

Carbanak C&Cs

hxxp://atlantis-bahamas[.]com/css/informs.jsp
hxxp://138[.]201[.]44[.]4/informs.jsp

Carbanak Cobalt Strike / Meterpreter DNS Beacon C&Cs

aaa.stage.15594901.en.onokder[.]com
aaa.stage.4710846.ns3.kiposerd[.]com