Analysis of the latest Emotet propagation campaign

By Diego Perez

ESET Research

An analysis of the workings of this new Emotet campaign, which has affected various countries in Latin America by taking advantage of Microsoft Office files to hide its malicious activity

28 Dec 2018 • , 3 min. read

In November, we issued warnings about a huge new spam campaign which was being used to propagate Emotet. Considering the scale of the attack in some Latin American countries and the fact that we received numerous inquiries about it over the last few days, we decided to publish a brief explanation of how this propagation campaign worked.

In recent years we have seen how cybercriminals have taken advantage of the Microsoft Office suite to propagate their threats, from simple macros embedded in files to the exploitation of vulnerabilities. On this occasion though, the implementation is a little unusual, consisting of a downloader incorporated into an Office file. This caused confusion among many users, who asked us to explain how the threat works.

The propagation began with an email message, which had nothing particularly special about it. As seen in Figure 1, it was pretty much the kind of email we are used to seeing in these campaigns.

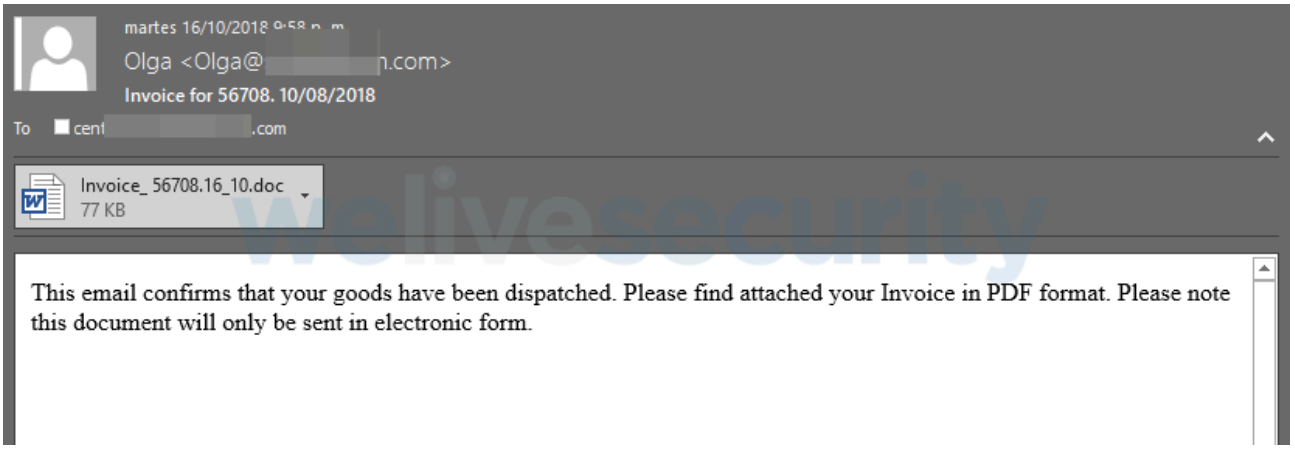

Figure 1 – A typical email from this Emotet campaign

As we might expect, if the user decides to download the email attachment and open the document, it asks them to enable the macros. Again, as is usual, some justification for this requirement is provided. Figure 2 shows that in this case it is implied this is necessary because the document was created using Office 365, but really it is so it can execute a function embedded in the file.

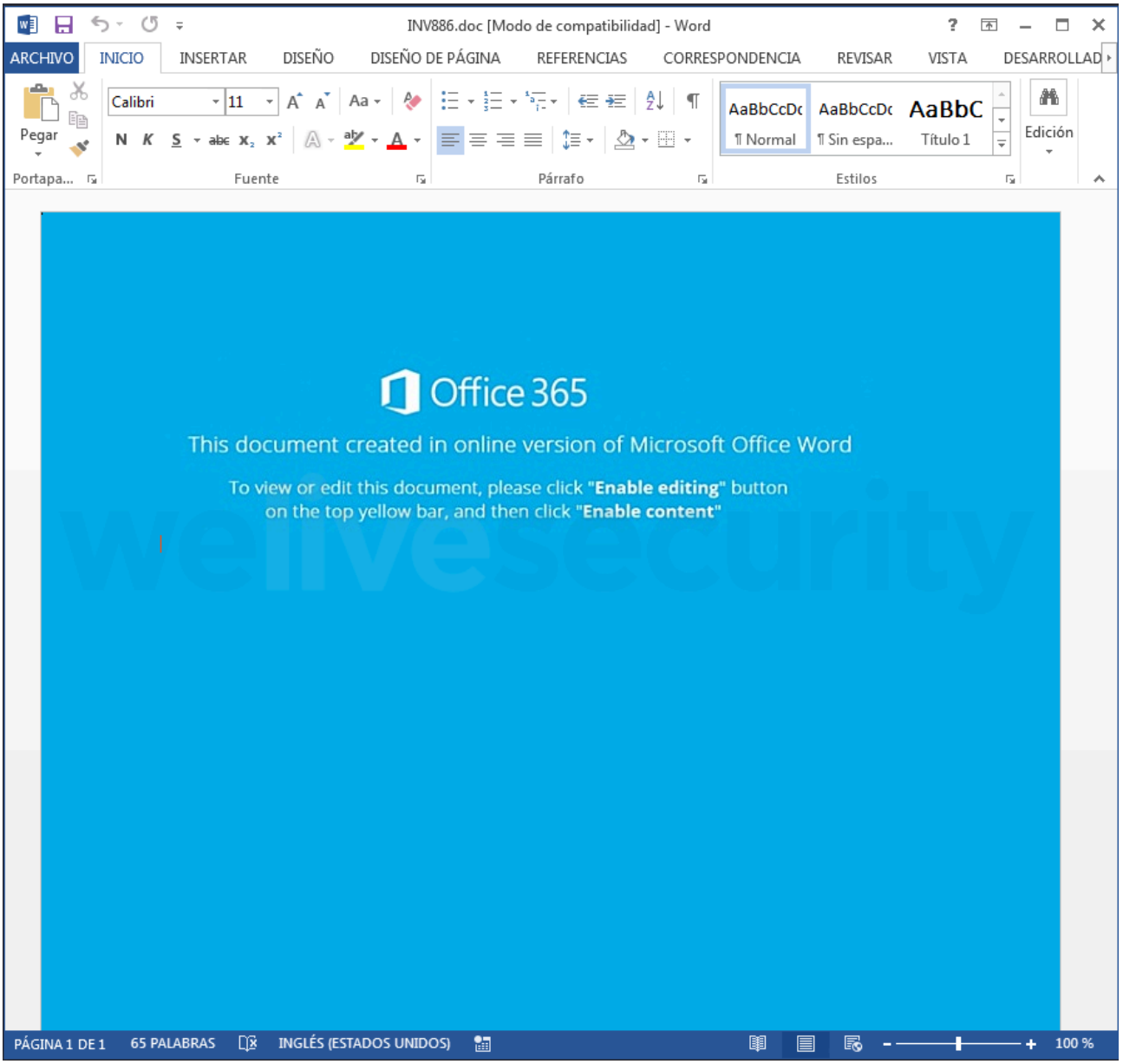

Figure 2 – Request to enable the document's macros

Clearly, this behavior is already known to be malicious. However, the trick used by the cybercriminals in this campaign has several unusual features. If you opt to look at the macro, you find that it is not very big and at first glance, it does not seem to be one of those known macros that try to connect to a website to download some content... or is it?

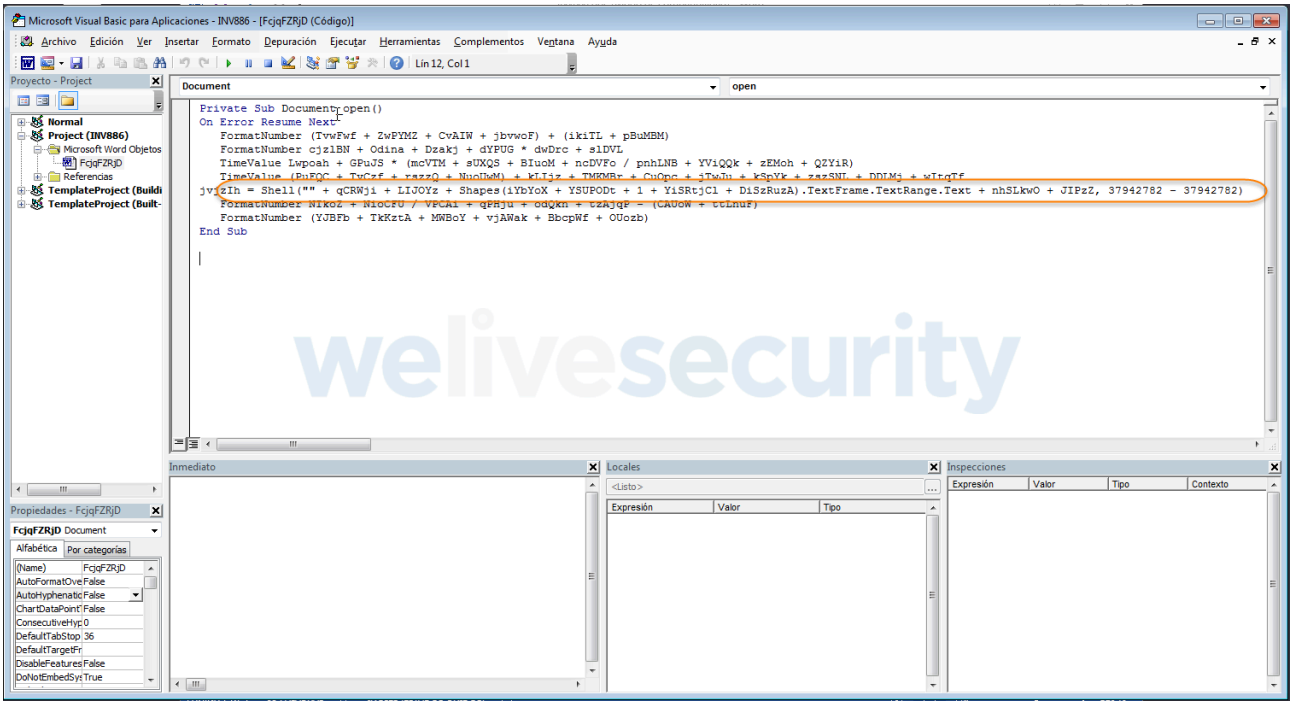

Figure 3 – The unusually compact VBA macro code in these documents

Looking at the macro, what stands out clearly is that its function is to read text from an object. But where is the object located? After searching for it, it turns out that there is an all-but-imperceptible object in the page. If you look closely at the top-left of the page in Figure 2, you will see what appears to be a very small, square, solid, black box. If you expand that, you can see what it contains.

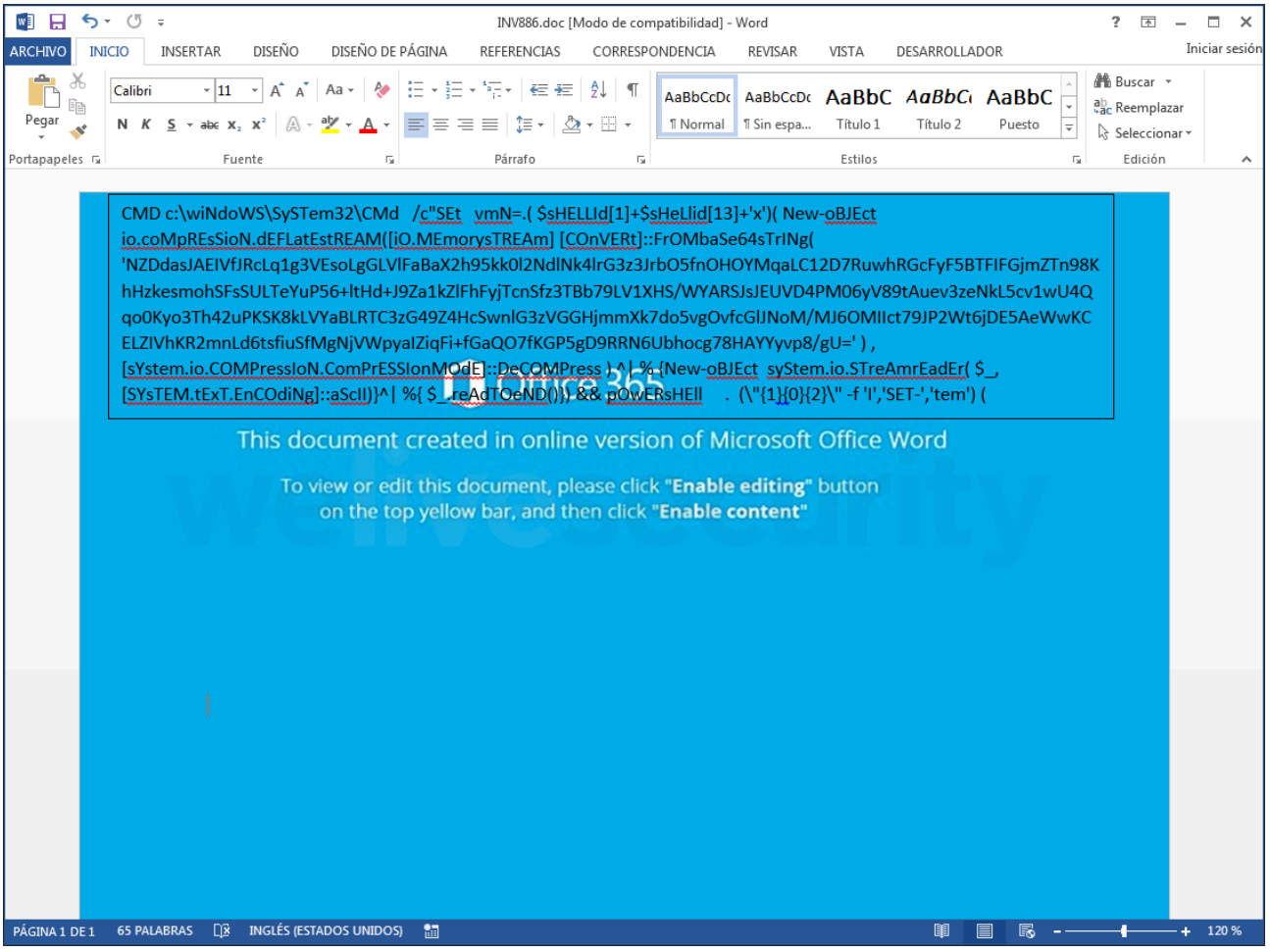

Figure 4 – Expanding the tiny object in the page to expose its contents

Effectively, this text box contains a "cmd" command, which launches a PowerShell script that tries to connect to five sites and then download the payload, which in this case is an obfuscated variant of Emotet.

As we have discussed in previous posts (for example, in this post from November 9), once the payload is executed, it establishes persistence on the computer and reports its success to its C&C server. Having completed this initial infection, further downloads can occur, installing attack modules and secondary payloads which carry out other kinds of actions on the compromised computer.

The various additional modules extend the range of malicious activities that can compromise the user's device, in order to steal credentials, propagate itself on the network, harvest sensitive information, carry out port forwarding, and many other possibilities.

Though not at all a new technique, this small change in the way *Emotet's* action is hidden within the Word file demonstrates how sneaky cybercriminals can be when it comes to concealing their malicious activity and trying to compromise user information. Staying in the know about the kinds of techniques they might use is always going to give the defenders an advantage in identifying these malicious campaigns.