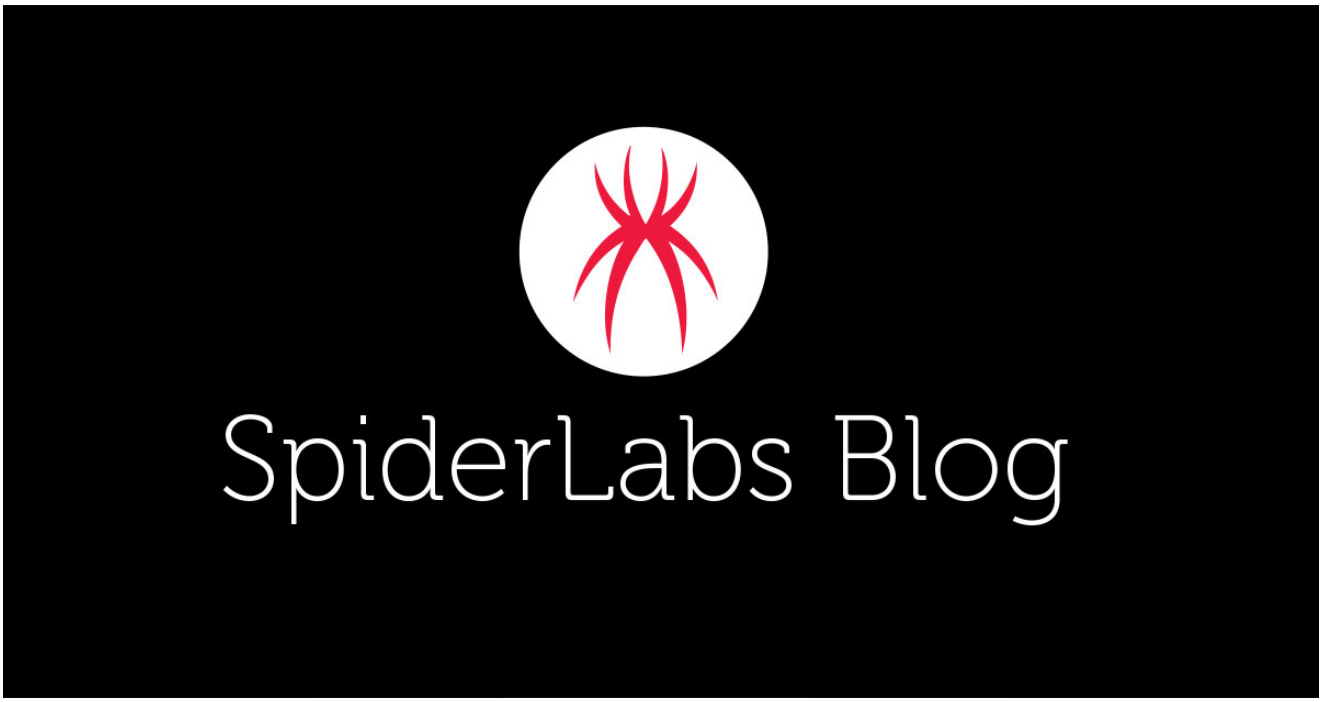
Trojanized OneNote Document Leads to Formbook Malware

trustwave.com/en-us/resources/blogs/spiderlabs-blog/trojanized-onenote-document-leads-to-formbook-malware/



Cybercriminals have long used Microsoft documents to pass along malware and they are always experimenting with new ways to deliver malicious packages. As defenders, Trustwave SpiderLabs' researchers are always looking out for new or unusual file types, and through this ongoing research, we uncovered threat actors using a OneNote document to move Formbook malware, an information stealing trojan sold on an underground hacking forum since mid-2016 as malware-as-a-service. Formbook malware can steal data from various web browsers and from other applications. This malware also has keylogging functionality and can take screenshots.

One file type that caught our eye on December 6, 2022, was the aforementioned OneNote attachment, with a .one extension attached to a spam email in our telemetry system. It's not typical to email .one files, so we took a closer look at the email, which is shown below.

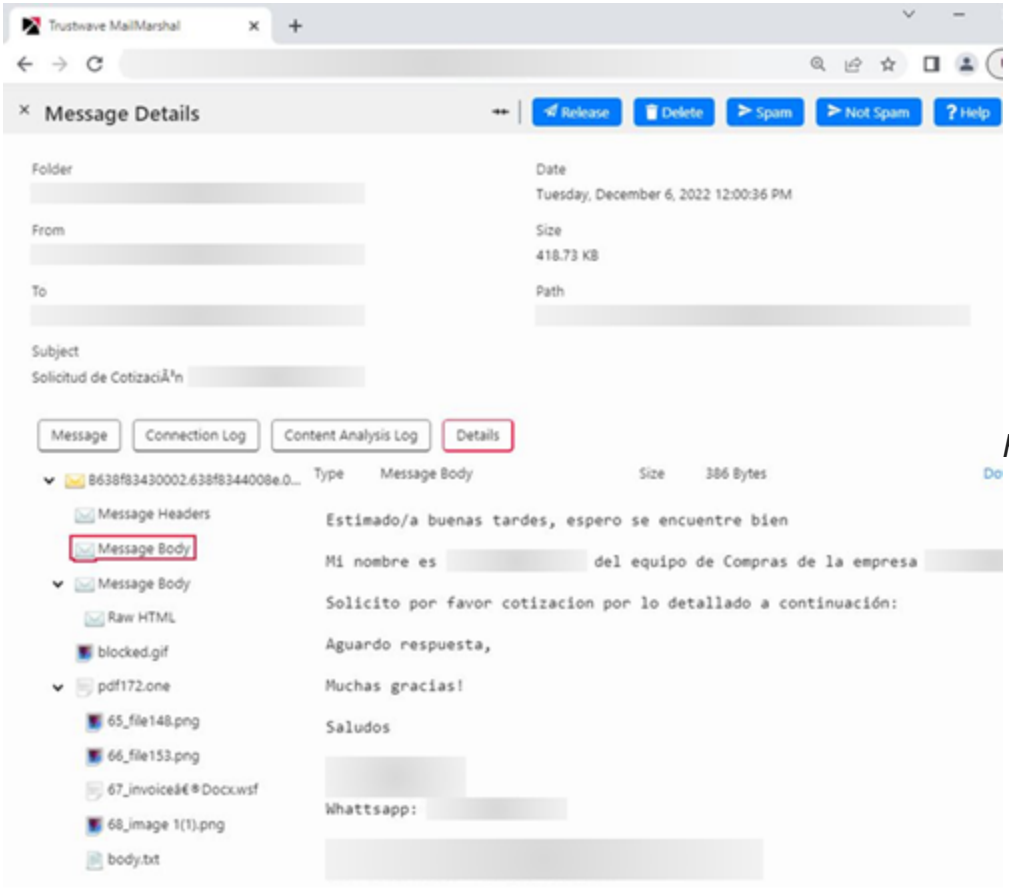


Figure 1: The email sample as viewed with the MailMarshal Console

Translation

Dear (client) Good Afternoon, I hope this finds you well.

My name is ___ from the Purchasing team at the ___ company.

Please provide a quote for the details below:

I await your reply,

Thank You Very Much!

Regards

Whatsapp:

Once the OneNote attachment is opened, an image lure is displayed. When the user clicks on the ‘View Document’ part of the image, a security warning appears.

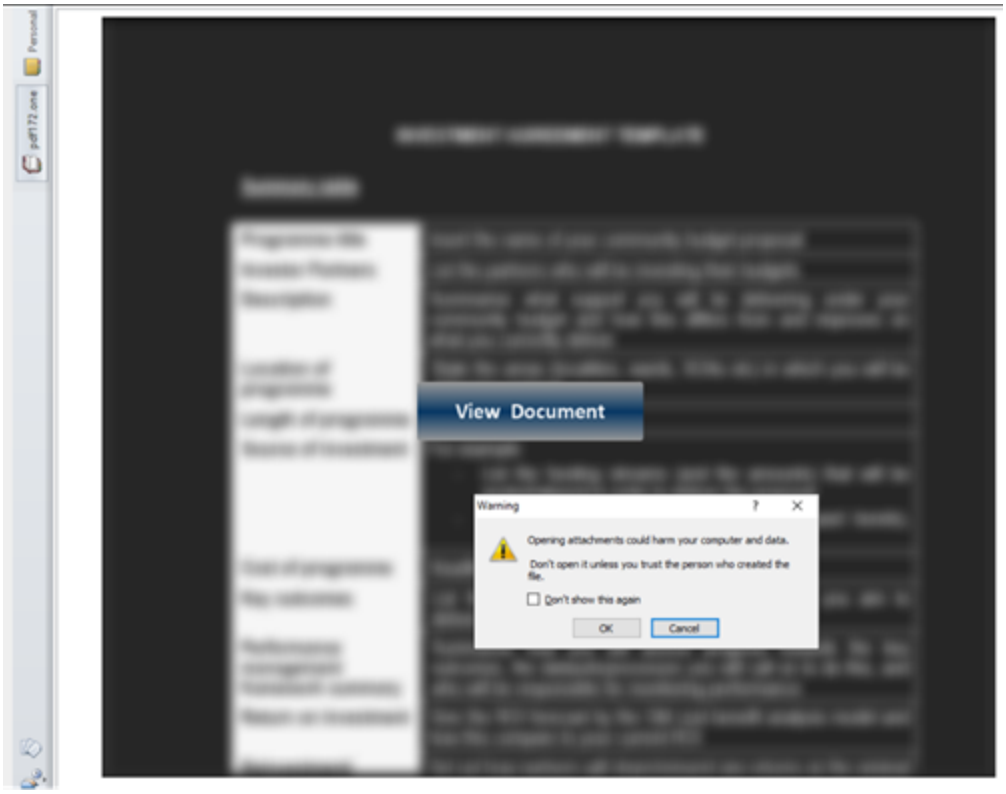


Figure 2: The attached OneNote file pdf172.one

As shown in Figure 1, MailMarshal's engine recognized and unpacked the contents of *pdf172.one*. One of the unpacked components is a Windows Script File (WSF), which is overlaid on the 'View Document' part of the image. When a user clicks on the 'View Document" part of the image, this causes the WSF file to be executed, and triggers a standard security alert that a file is being opened from the OneNote application.

Also, it is interesting that the filename of the WSF itself has some deception, likely an attempt to fool scanners. The filename contains a right-to-left override character (U+202E) after 'invoice', which causes the text that follows to be displayed in reverse. So, instead of displaying 'docx.wsf' some applications may display 'fsw.xcoD'.

When a user clicks on the 'View Document" part of the image, this causes the WSF file to be executed, and triggers a standard security alert that a file is being opened from the OneNote application.

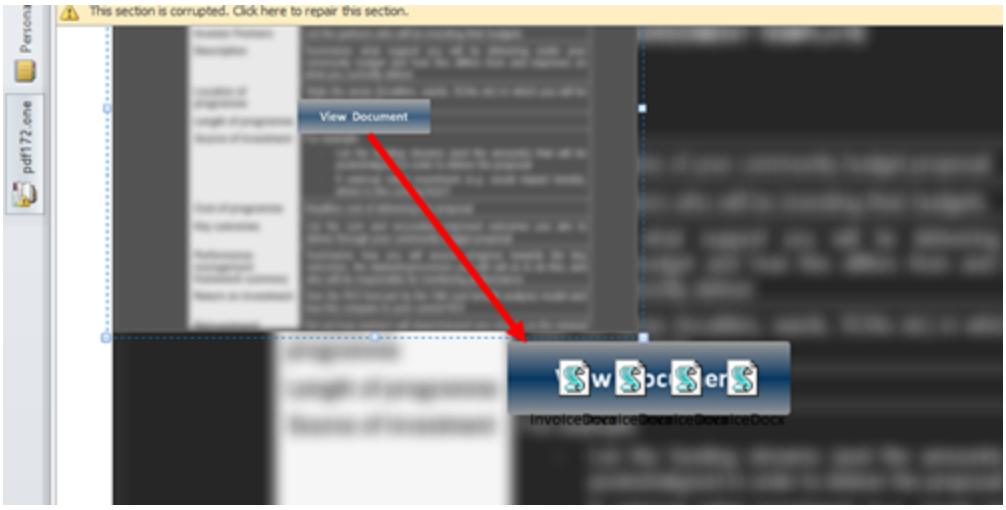


Figure 3: The WSF file overlayed to the lure image

When the user goes against the warning and clicks 'OK,' the malicious behavior of the file will start to manifest. The WSF embedded in the OneNote file launches 'PowerShell' commands to download and execute two files from *a0745450[.]xsph[.]ru*.

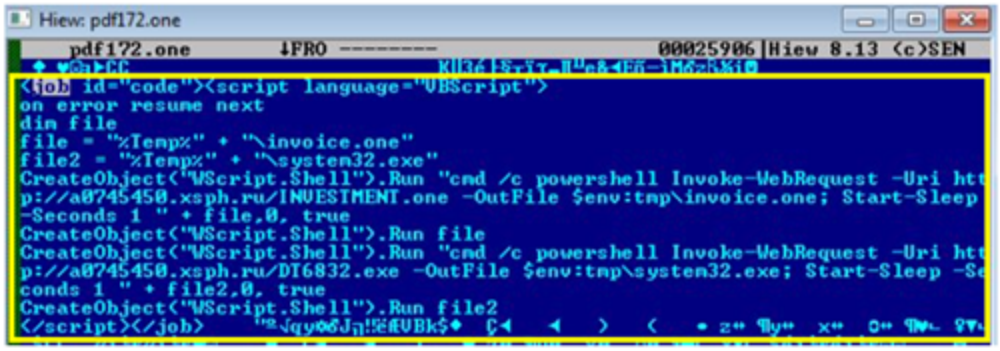


Figure 4: The WSF contained on the OneNote attachment

The first file to be retrieved is a decoy OneNote file. This will be downloaded from *a0745450[.]xsph[.]ru/INVESTEMENT[.]one* and saved as *%temp%\invoice.one*. The decoy file will be launched first to hide the downloading of the second file, which contains the payload.

The second file is an executable which will be downloaded from *a0745450[.]xsph[.]ru/DT6832.exe* and saved as %temp%*system32.exe*. This executable is the Formbook malware, an information stealing trojan sold on an underground hacking forum since mid-2016 as malware-as-a-service. Formbook malware can steal data from various web browsers and from other applications. This malware also has keylogging functionality and can take screenshots.

In sum, a WSF file embedded in a OneNote document is likely to fly under the radar. It also means that OneNote can now join the list of other Office Documents that need to be inspected for malicious components. As mentioned earlier, it's not typical to see .one files

attached to emails. As a mitigation step, organizations should consider blocking or flagging inbound email attachments with a .one extension.

For Trustwave MailMarshal customers: Upon detecting this threat, the Trustwave SpiderLabs' MailMarshal Team released extra heuristics for characteristics of the *.one* malicious attachment.

IOCs

Hashes

Pdf172.one (306792 bytes)
81bd8c431811f83f335735847d42fb4f64f80960 (SHA1)

DT6832.exe (218925 bytes)
d5ee9183be486bf153d7666ca4301e600ea06087 (SHA1)

INVESTMENT.one (59472 bytes)
33d8fb75f471bdc4ebaff053e87146721f32667a (SHA1)

URLs

a0745450[.]xsph[.]ru/DT6832[.]exe

a0745450[.]xsph[.]ru/INVESTEMENT[.]one