Purchase Order Phishing, the Everlasting Phishing Tactic

cofense.com/purchase-order-phishing-the-everlasting-phishing-tactic/

Cofense October 27, 2020

Phish Found in Environments Protected by SEGs

Mimecast

Microsoft EOP

Microsoft ATP

By Adam Martin, Nathaniel Sagibanda, Kian Buckley Maher and Cofense Phishing Defense Center

The PDC team has seen a recent up-tick in legitimate Mimecast services being used as a vector for phishing campaigns found in environments protected by Microsoft ATP, Microsoft EOP and Mimecast.

The phish leverage the “Payment Order,” a common vector for enticing users into initiating the process set out by a malicious actor to attain sensitive credentials (Figure 1).

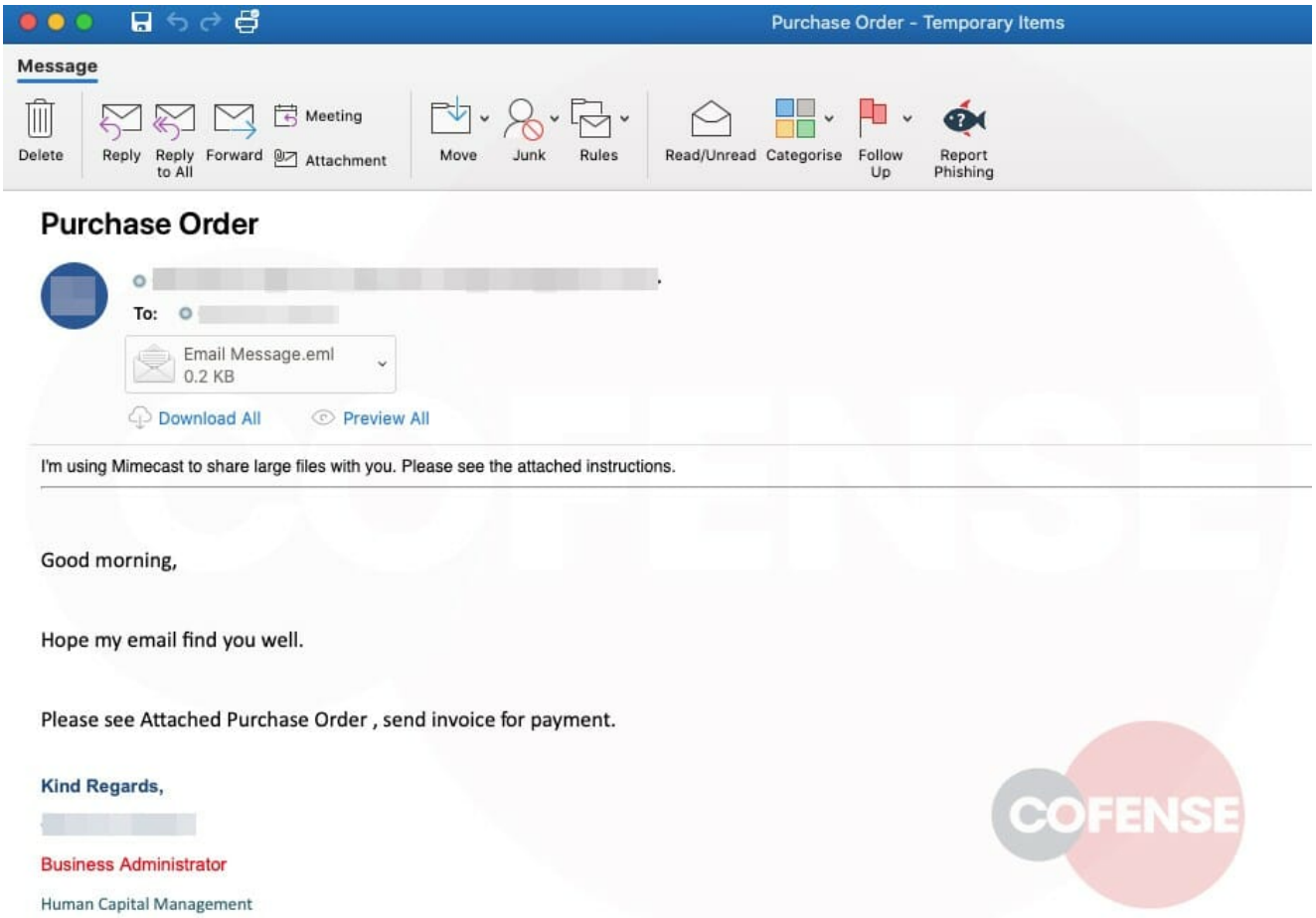

Figure 1

In this attack, as illustrated in figures, the body of the email is a reasonable facsimile of an authentic message that even replicates the style of the Mimecast heading and disclaimer. But grammatical, punctuation and spacing anomalies represent red flags. Furthermore, the email itself looks benign, simple and straight to the point, informing the recipient that the required information is behind an external service due to an issue with storage size or formatting (Figure 1). This is a common tactic that allows malicious actors to circumvent mail filters such as Mimecast, Microsoft EOP and Microsoft ATP.

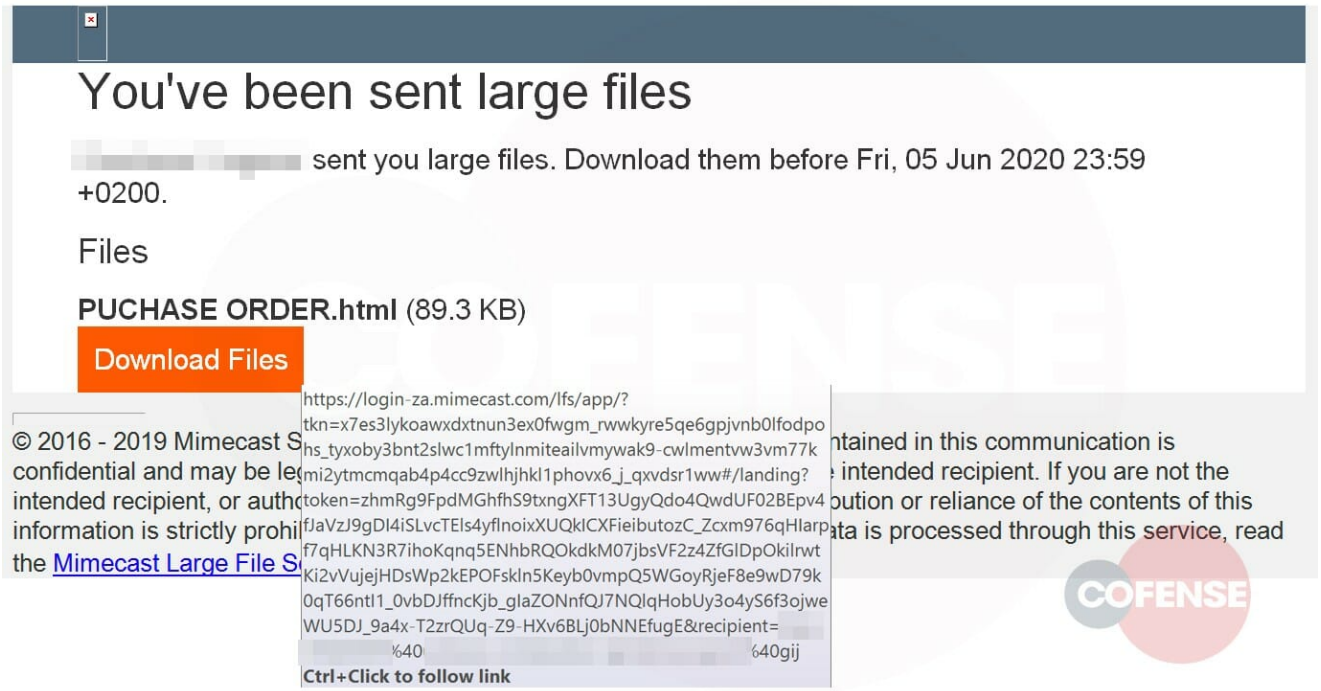

Figure 2

Upon inspection of the “Download Files” button we can see that the service being used to deliver this phish is in fact Mimecast, itself a legitimate service. Combining this with the previously noted circumvention method makes standard detection almost impossible.

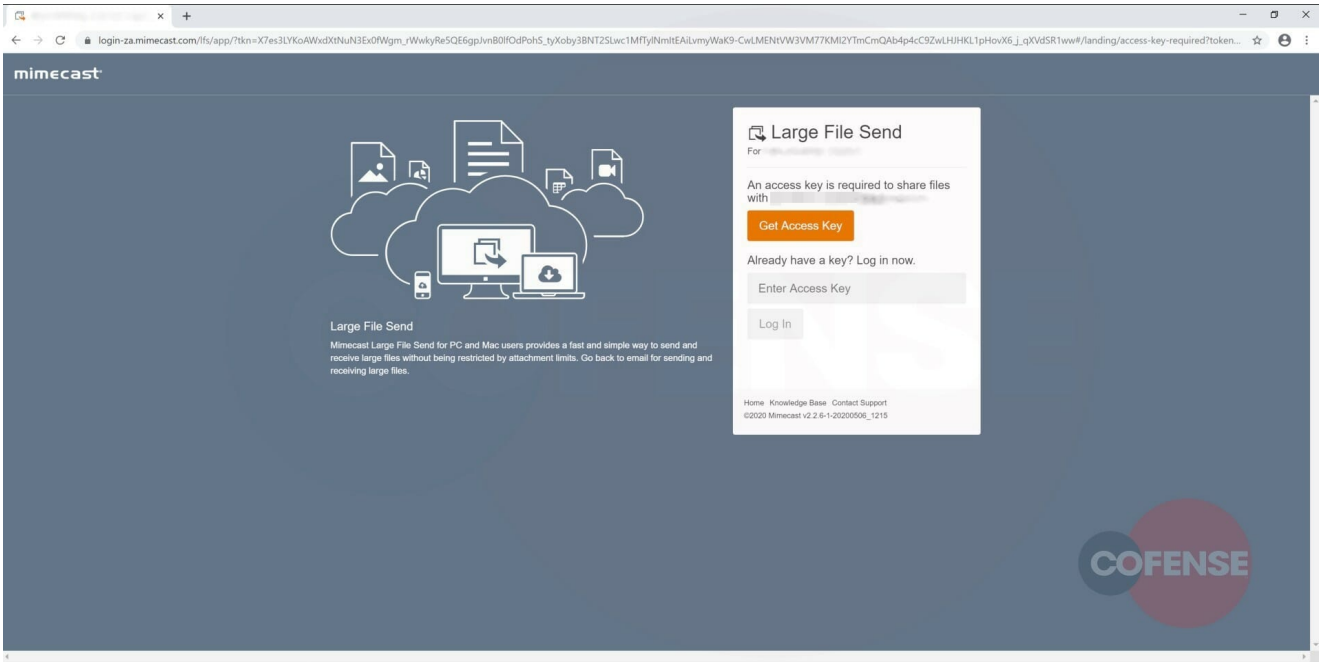

Figure 3

As seen in Figure 3, the page presented to the user is a legitimate Mimecast service being used to host the malicious file. This is compounded by the use of a key to gain access to the file by clicking the access-key button or entering a previously provided key (see Figure 3). However, both methods will direct the user to the next stage.

Once access has been gained to the first landing page, there will be an option to download the malicious file at the side of the page. To add authenticity, the credentials of the original sender have been replicated, as shown below in Figure 4.

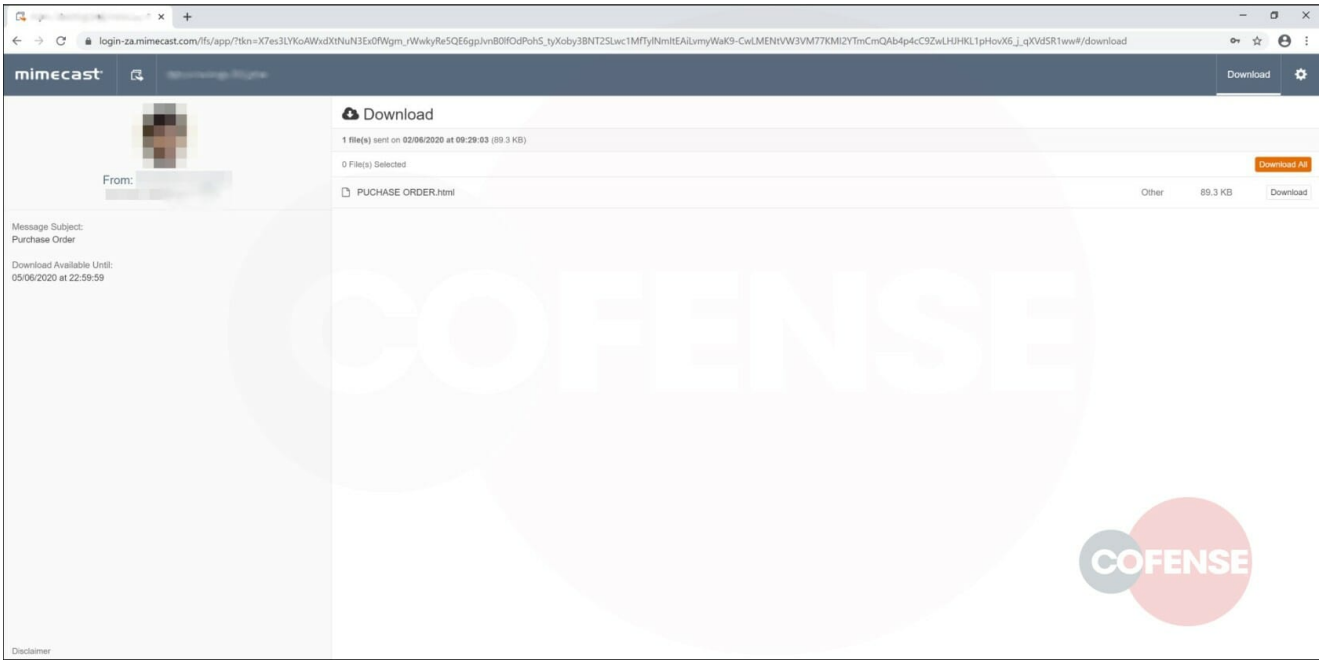

Figure 4

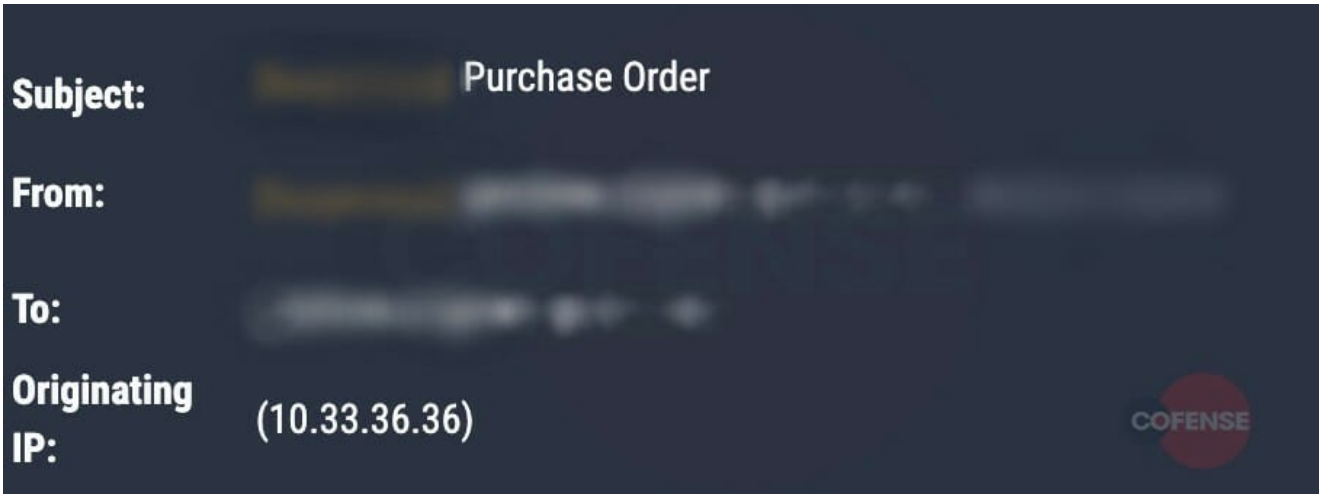

Figure 5

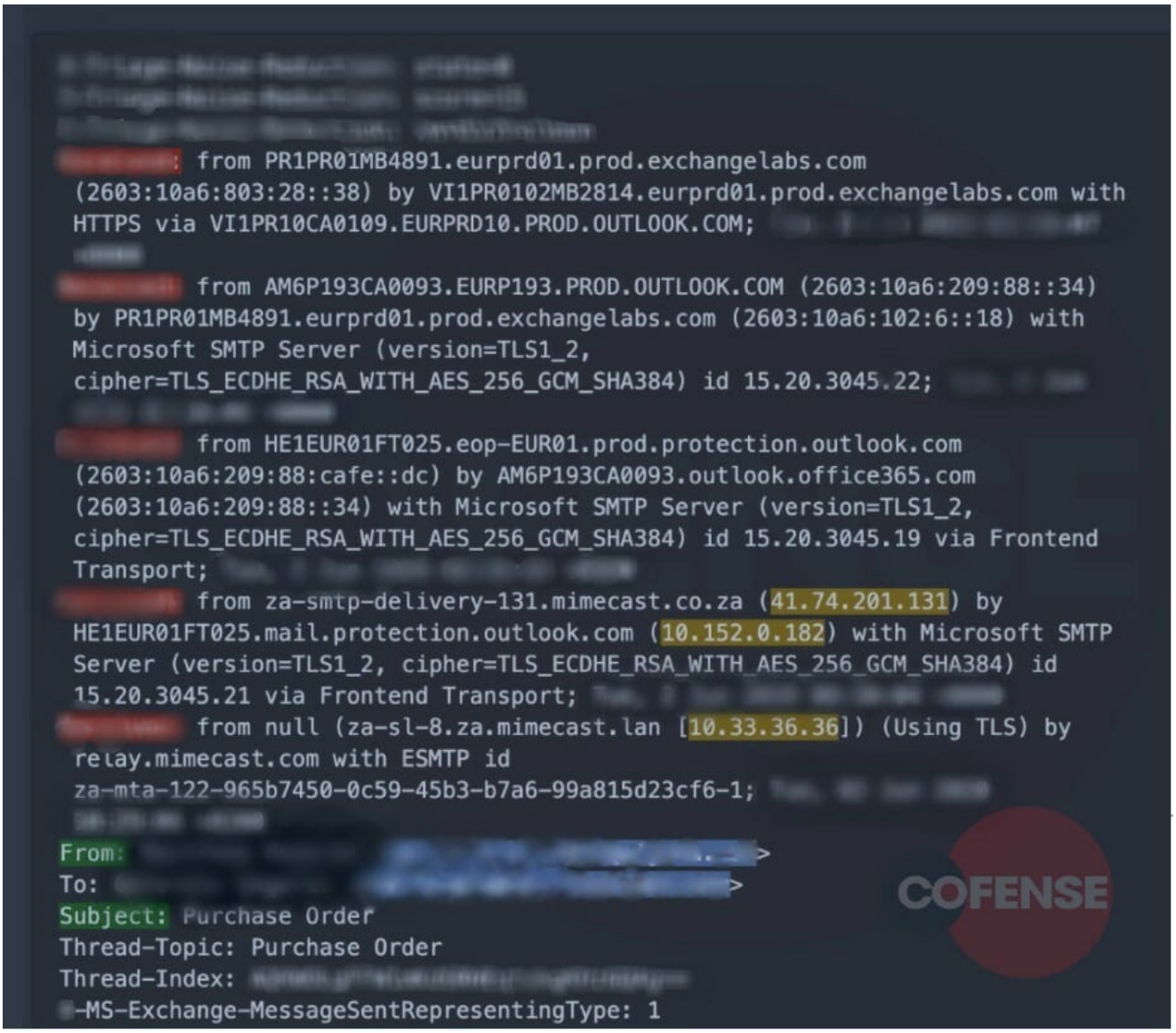

Figure 6

Email Header analysis: Taking a look at the headers on Figure 6, it is a different story altogether. IP addresses such as [10.x.x.182 and 10.x.x.36] are used by independent operating networks. These may be as small as a single computer connected to a home gateway, and are installed in hundreds of millions of devices automatically.

However, IP 41.x.x.131 belongs to MimecastSA (according to VirusTotal and Whois), and could be the reason it escaped SEG detection.

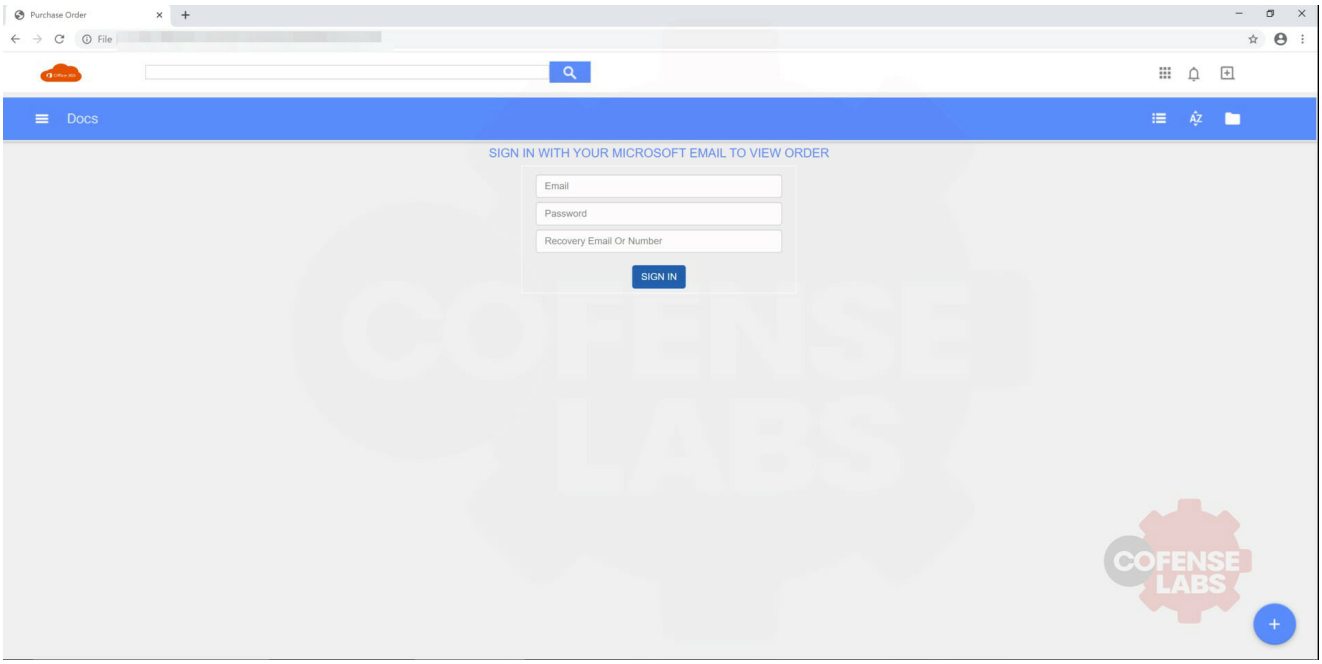

Figure 7

Having accessed the malicious link, the user will see the above page displayed (Figure 7) with a request for the user's Microsoft email address and password. Unlike other credential phishing pages, the Microsoft background and logo aren't displayed. The simplicity of the page, combined with a URL lacking indicators of Microsoft or associated domains, is suspect. The third field is the most obvious red flag (Figure 7): A recovery option is made available even though an incorrect password hasn't been entered. This is done to prompt the victim into providing a phone number.

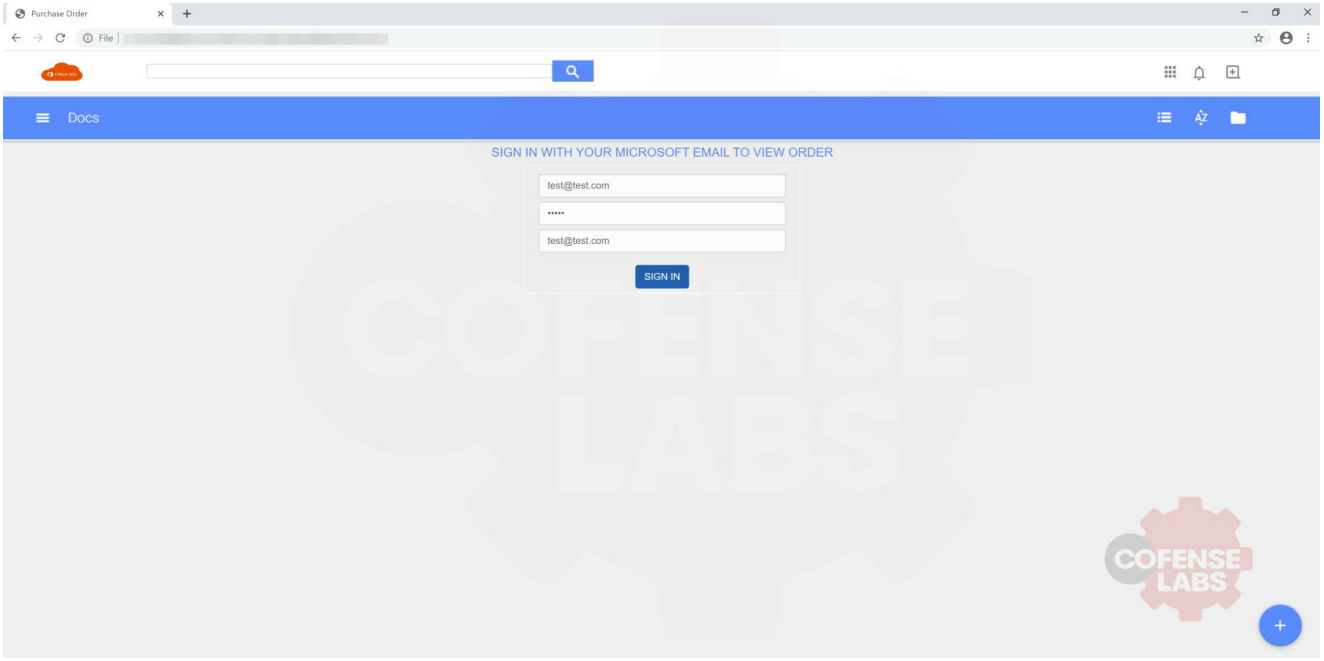

Figure 8

Having inserted test credentials, the information is exported to the phishing campaign URL address. This site is hosted by hxxps://www.docdroid[.]net/OwKxXnZ/purchase-order-00177389-pdf. Entering information will continually refresh the page regardless of credentials supplied.

Indicators of Compromise

Network IOC	IP
hXXp://biz267.inmotionhosting[.]com/~craneo5/pow/po[.]php	23[.]235[.]212[.]50
hXXps://www.docdroid[.]net/OwKxXnZ/purchase-order-00177389-pdf	54[.]37[.]79[.]95

Don't miss out on any of our phishing updates! Subscribe to our blog.