Threat Actor Utilizes COVID-19 Uncertainty to Target Users

cofense.com/threat-actor-utilizes-covid-19-uncertainty-to-target-users/

Cofense November 19, 2020

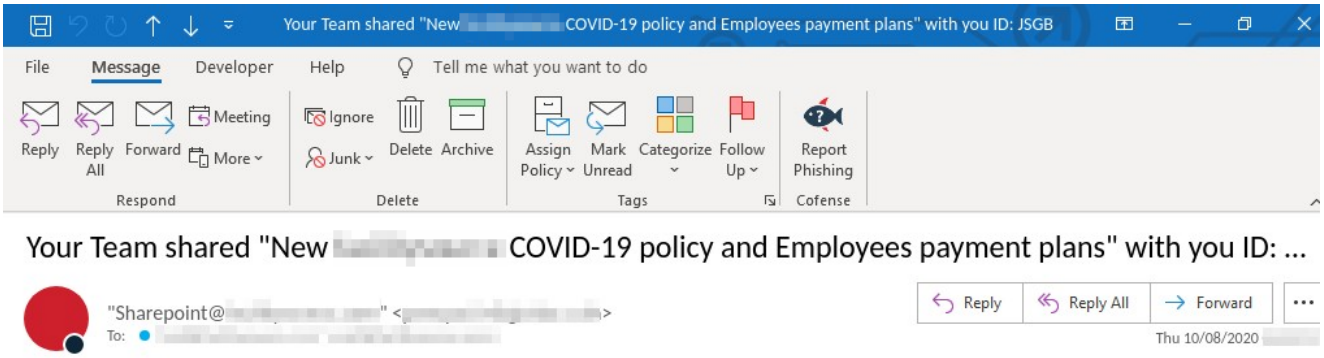
Phish Found in Environments Protected by SEGs

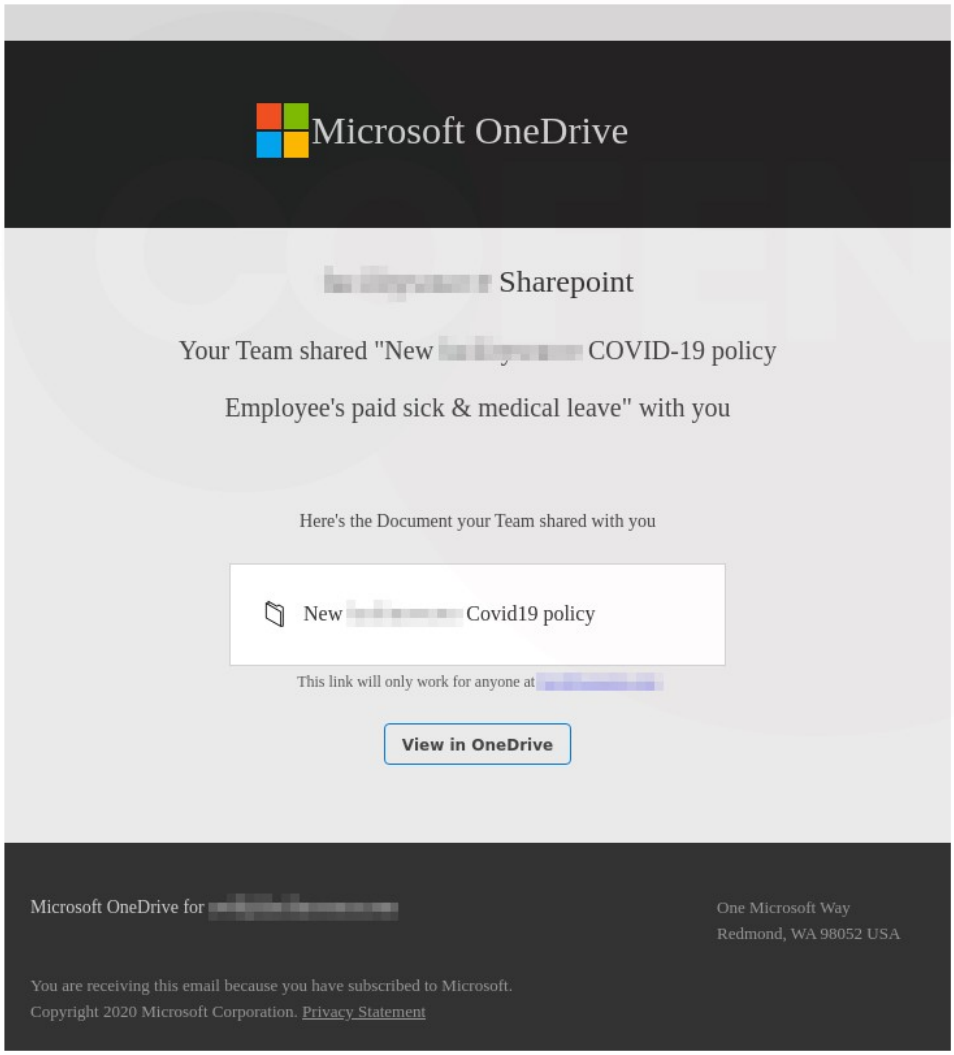
Proofpoint

By Kyle Duncan, *Cofense Phishing Defense Center*

As the world continues to contend with a tenacious pandemic, many employers are obliged to revisit medical-benefit policies. The Cofense Phishing Defense Center (PDC) has observed a new phishing campaign that aims to harvest Microsoft login credentials by posing

as a company-wide sick/medical leave policy update.





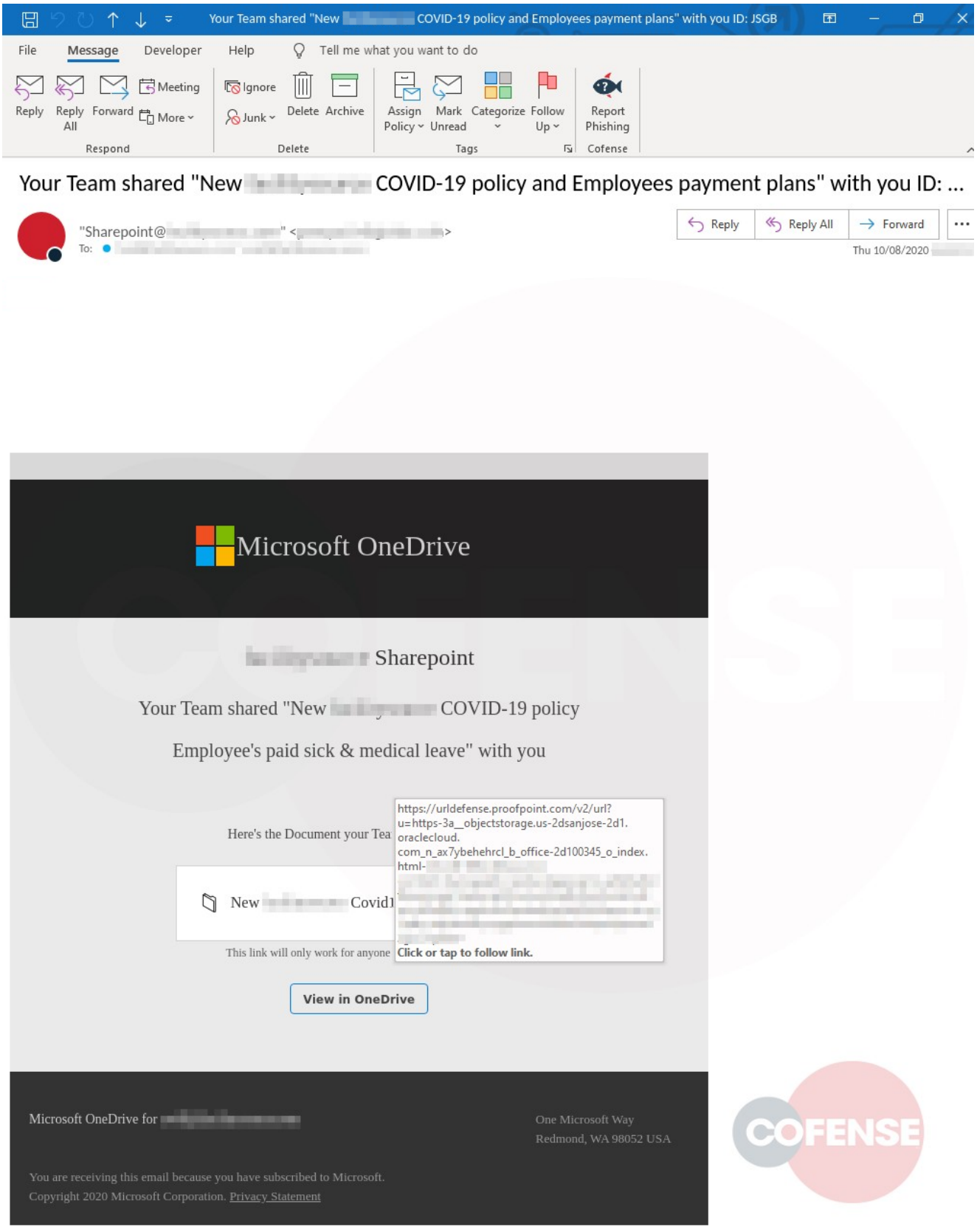


Figure 1-2: Email Body

The sender's email address is spoofed to appear as though the email is originating from the company's SharePoint services by using the format "Sharepoint@[companyname].com". However, one look into the email's header information shows that this is not the case and that the email originated from outside of the organization, potentially from a compromised account operated by the threat actor.

The email body itself is put together well and, at a glance, appears as though it could be legitimate. It even contains little details such as "This link will only work for anyone at [company name]" and "Microsoft OneDrive for [user's email]." The threat actor has spoofed a legitimate Microsoft notification to appear legitimate, using a format the recipient would quickly trust at first glance. Since the file being shared refers to the company's approach on sick leave during COVID-19, users are naturally going to be curious about what their company is doing for them.

The glaring flaw with the email body is where it references both Microsoft OneDrive and SharePoint. Since the spoofed email address is attempting to trick the user into thinking this is a shared SharePoint file, it does not make sense for the email body to reference both of these services. It thus raises suspicion. The button users are intended to click also references OneDrive and, hovering over it, it reveals that the domain of the destination (oraclecloud[.]com) has nothing to do with Microsoft. It is apparent that this is not what it claims to be.

Upon visiting the malicious URL, users are taken to a fake Microsoft login page as shown in Figure 3.

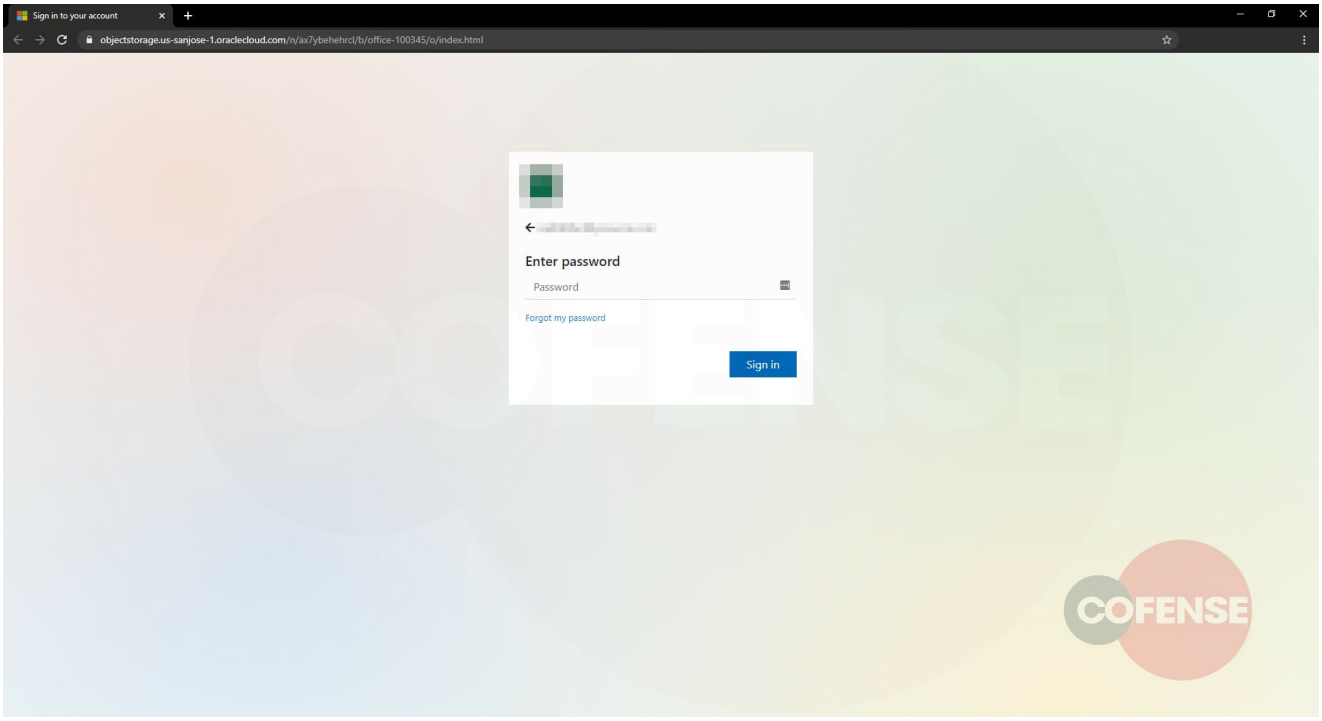


Figure 3: Phishing Page

The email address field of the login is automatically populated with the user's email so they would only have to include their password. The page even includes the company's logo to more effectively pass the login off as legitimate. Once the credentials have been secured, the user is then redirected to a page containing COVID-19 documentation, as seen in Figure 4, that seemingly appears relevant to what was mentioned in the email. While many phishing attempts redirect the user to a legitimate login page, the use of this document instead is another attempt to prevent the realization that the user's credentials were just stolen.

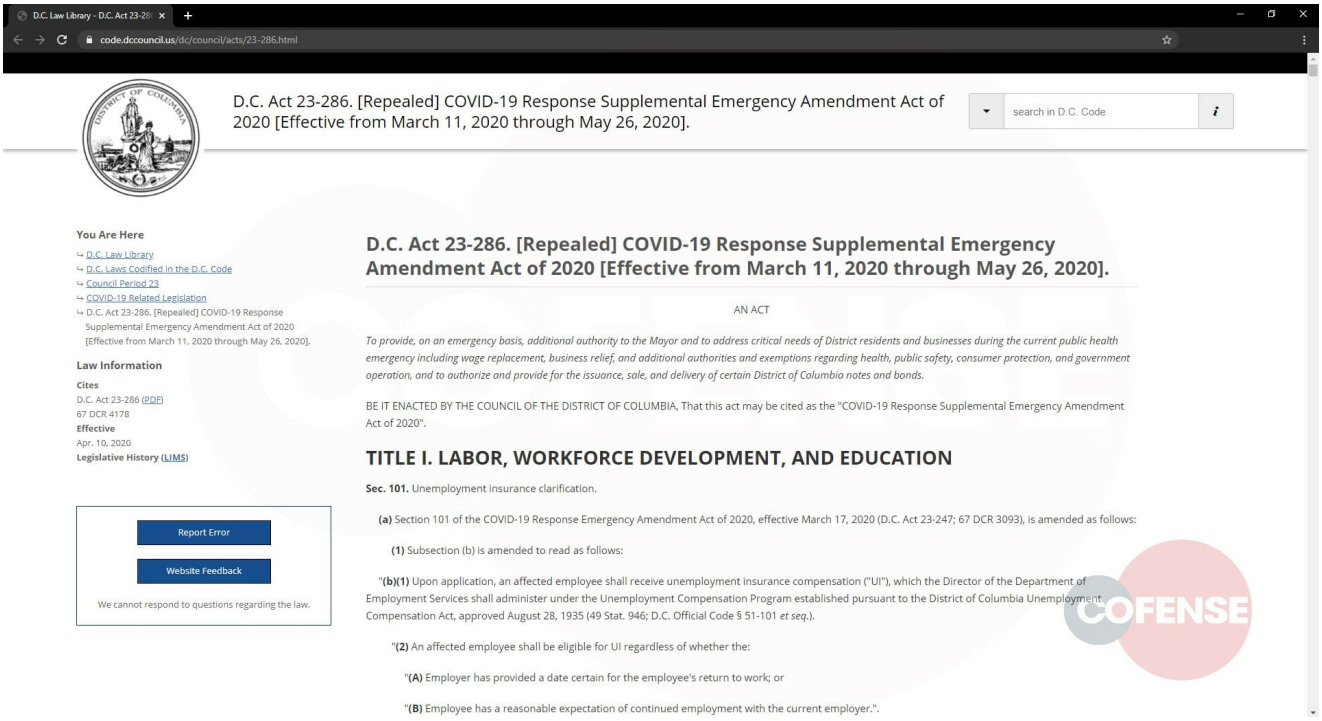


Figure 4: Final Redirect Page

Indicators of Compromise

hXXps://objectstorage[.]us-sanjose-1[.]oraclecloud[.]com/n/ax7ybehehrcl/b/office-100345/o/index.html	134[.]70[.]124[.]2

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