Cybersécurité : comment les ouragans déclenchent aussi des cyberattaques

Comme souvent lors d'événements majeurs qui attirent l'attention du public, les chercheurs de Proofpoint ont observé un certain nombre de leurres de phishing exploitant l' ouragan Michael. Cependant, alors que les programmes de phishing liés aux catastrophes naturelles tentent souvent de voler des numéros de carte de crédit utilisés pour de faux dons ou de voler des fonds directement via des dons frauduleux, bon nombre de ces campagnes récentes étaient axées sur le vol de identifiants par courrier électronique.
Il est intéressant de noter que les campagnes ont également exploité le stockage d'objets blob sur l'infrastructure Microsoft Azure pour héberger à moindre coût des modèles de phishing.

Campagnes de phishing
Un grand nombre des récentes campagnes de phishing avec les leurres « Hurricane Michael » ont utilisé des documents PDF joints à un courrier électronique. Ils incluent des noms de fichiers tels que:

- florida hurricane michael emergency and recovery procurement.pdf
- florida hurricane michael emergency and disaster recovery procurement.pdf
- vdot hurricane michael emergency and recovery procurements.pdf

Comme le montrent les figures 1 et 2, les leurres sont assez génériques et reposent sur des liens intégrés et une ingénierie sociale pour inciter les destinataires à cliquer. Les deux captures montrent des marques volées de vraies agences gouvernementales.

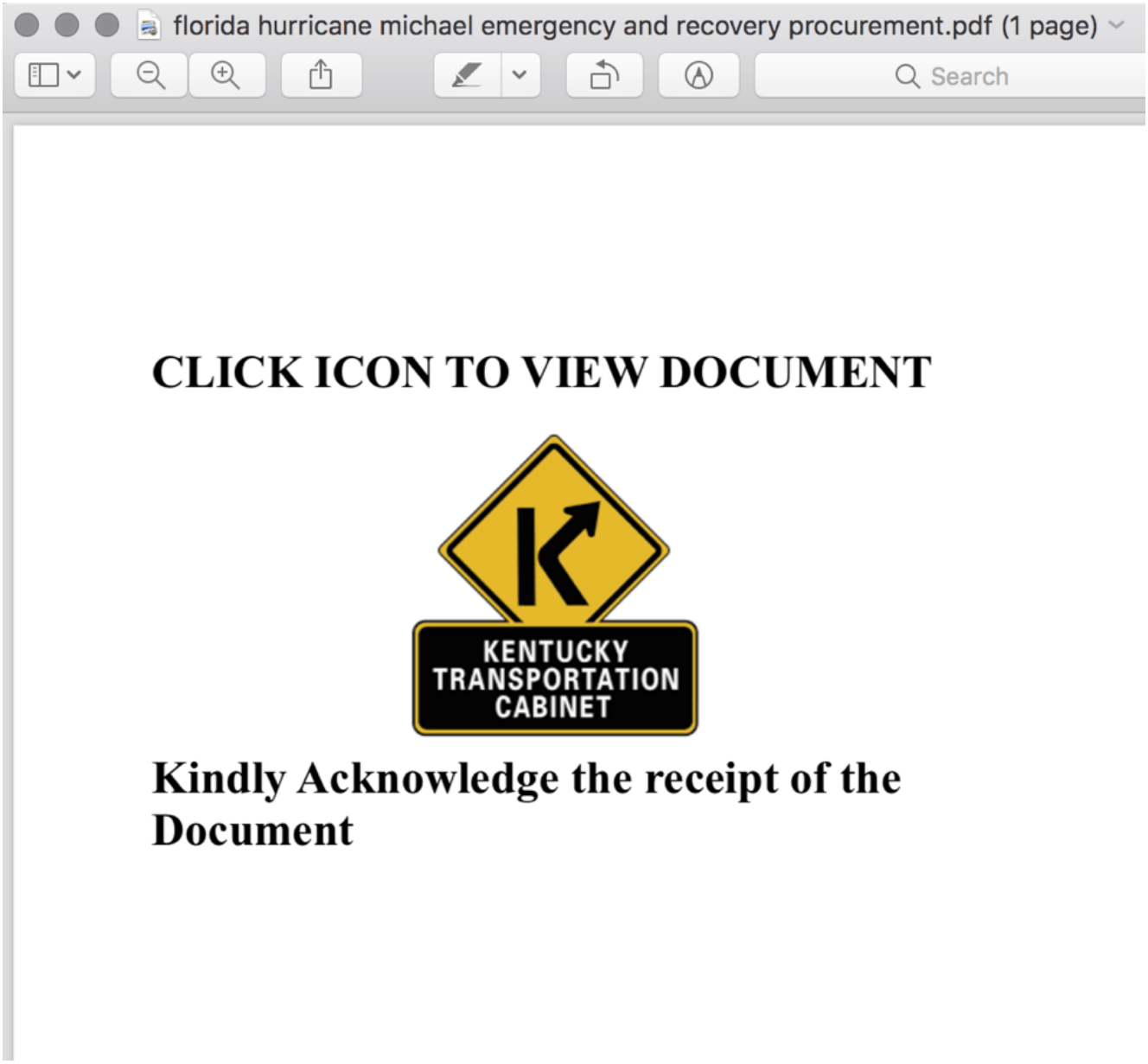

Figure 1: Un leurre PDF avec un lien intégré et une marque volée (Cabinet de transport du Kentucky)

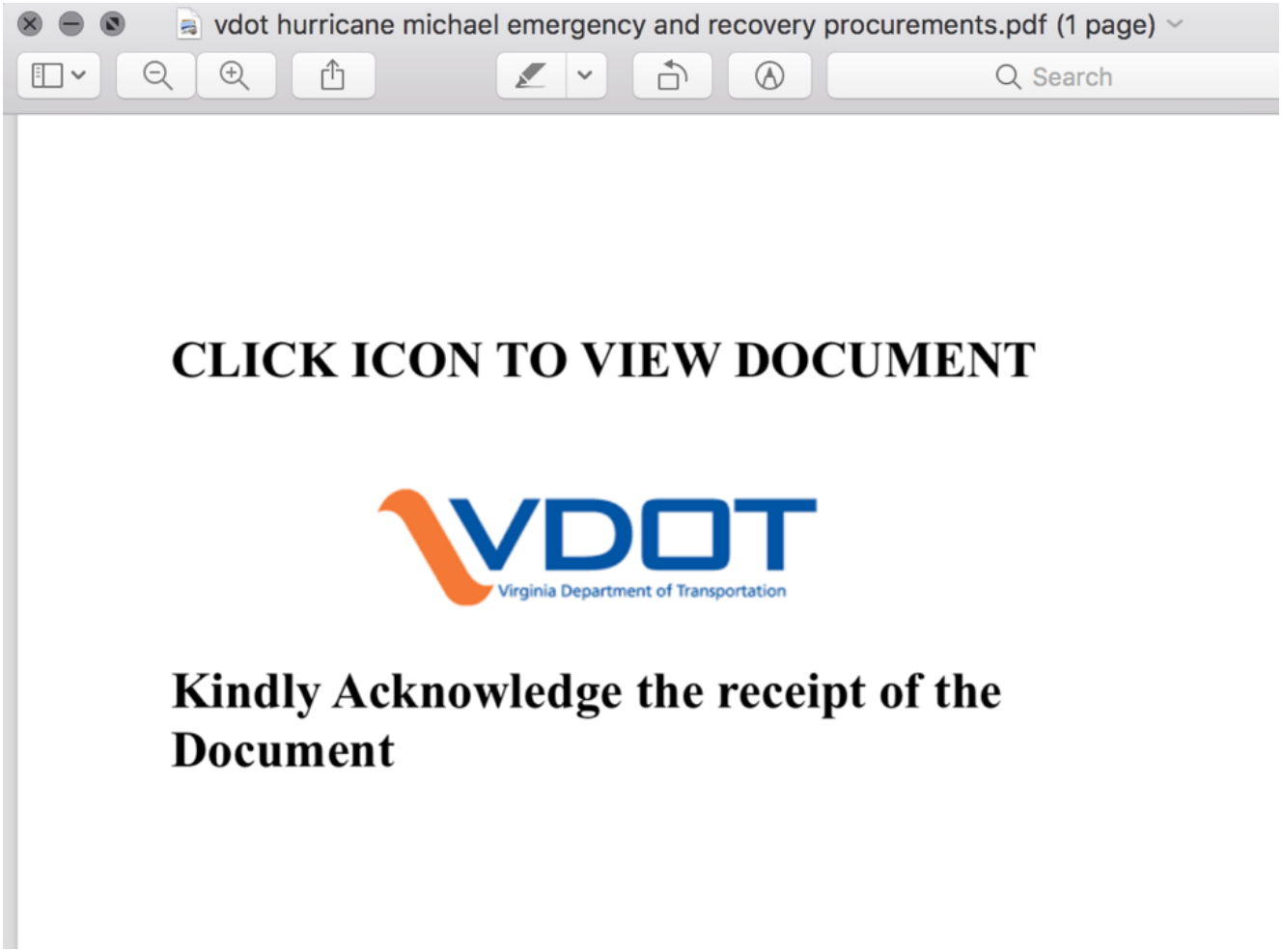

Figure 2: Un autre leurre PDF avec un lien intégré et une marque volée (Virginia Department of Transportation)

En cliquant sur les icônes liées, un lien bit.ly (raccourcisseur de lien) apparaît, puis le dernier lien vers la page de destination du phishing.

Les taux de clics semblent relativement faibles pour ces liens, avec un peu plus de 500 clics pour les trois URL observées associées à cette campagne (Figure 3).

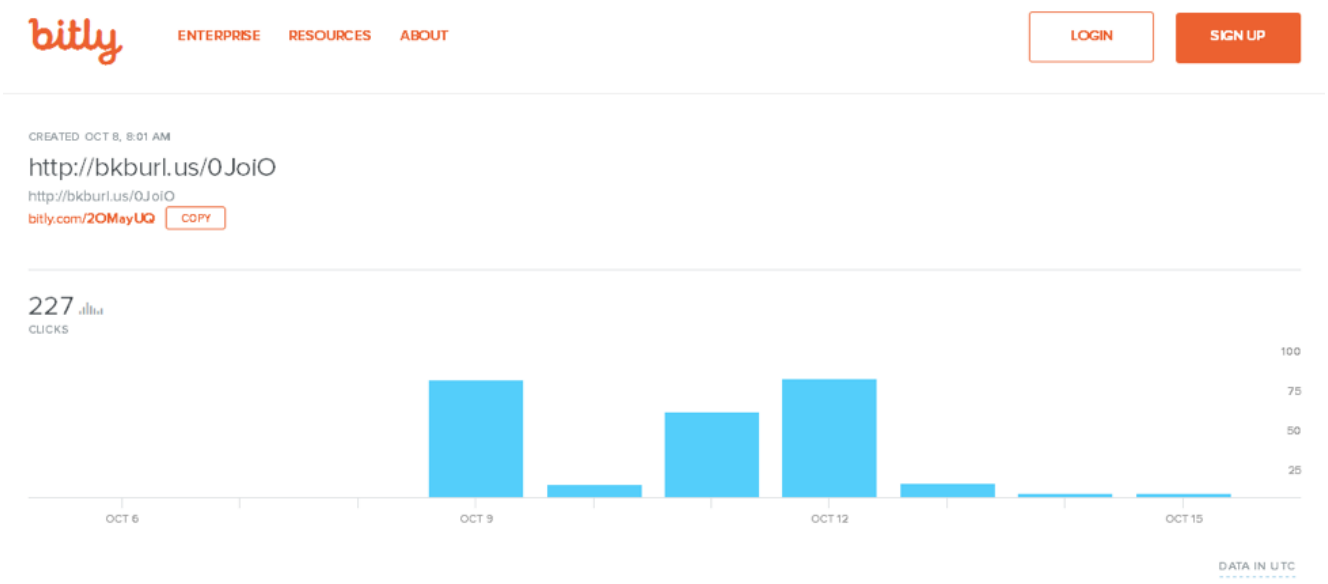

Figure 3: Statistiques concernant les clics sur les liens des PDF associés à ces campagnes de phishing

Malgré les faibles taux de clic globaux, toutefois, les URL finales présentent un intérêt:

- https: [//] dropboxembright19604.blob.core.windows [.] net
- https: [//] onedriveunfragrant26.blob.core.windows [.] net
- https: [//] onedrivechowry495462.blob.core.windows [.] net

Il s'agit de pages de phishing HTTPS uniquement et hébergées sur des domaines Windows [.] Net officiels. Nous observons des pages de phishing hébergées Microsoft Azure blob storage depuis août de cette année. Cette tactique est peu coûteuse et particulièrement efficace pour les escroqueries prétendant être des services Microsoft légitimes.

Le champ CommonName du certificat SSL / TLS présent dans ce cas est un certificat générique qui ne peut pas être utilisé comme moyen de détection efficace, comme le montre la figure 4. Il existe d'autres moyens de détecter l'activité malveillante, tels que les requêtes DNS en inspectant le TLS. indication du nom du serveur.

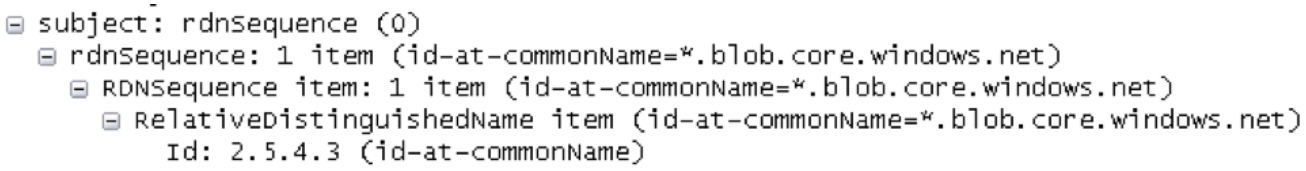

Figure 4: Certificat générique émis pour tous les domaines (bons et mauvais) sur ce domaine

Parmi les autres domaines d'hameçonnage récemment observés qui abusent de l'hébergement blob de Microsoft Azure, citons:

- 14 oct 2018 dropboxmarling951049.blob.core.windows [.] Net
- 12 oct 2018 cs7a779f8678a3dx443cxbf5.blob.core.windows [.] Net
- 12 octobre 2018 onedrivedocument3.z13.web.core.windows [.] Net
- 11 octobre 2018 krdas56-secondary.z19.web.core.windows [.] Net
- 11 octobre 2018 excelouttravel858824.blob.core.windows [.] Net
- 11 octobre 2018 onedrivemyliobatoid4.blob.core.windows [.] Net
- 11 octobre 2018 onedrivemoton8532961.blob.core.windows [.] Net
- Oct 11 2018 godaddyreimplant9949.blob.core.windows [.] Net
- 11 octobre 2018 onedrivedocs3.z13.web.core.windows [.] Net
- 11 octobre 2018 onedrivedocument0.z13.web.core.windows [.] Net
- 11 octobre 2018 onedrivebroadwayite7.blob.core.windows [.] Net
- 10 oct. 2018 office365totalized87.blob.core.windows [.] Net
- 10 octobre 2018 darkcloud.z13.web.core.windows [.] Net
- 10 oct 2018 ducosignsurahs721013.blob.core.windows [.] Net
- 10 oct 2018 dropboxsphingurus894.blob.core.windows [.] Net
- 10 oct. 2018 adobeadvanceable4826.blob.core.windows [.] Net
- 10 octobre 2018 onedriveexactas84338.blob.core.windows [.] Net
- 9 oct 2018 henricocountyassiste.blob.core.windows [.] Net
- 9 oct 2018 office365parasyphilo.blob.core.windows [.] Net
- 9 oct 2018 office365funguses335.blob.core.windows [.] Net

- 9 oct 2018 adobeinthralls778398.blob.core.windows [.] Net
- 9 octobre 2018 onedrivenonalphabeti.blob.core.windows [.] Net
- 9 oct 2018 ducosignunkept514717.blob.core.windows [.] Net
- 9 octobre 2018 onedriveunfragrant26.blob.core.windows [.] Net
- 9 octobre 2018 onedrivesuiogothic82.blob.core.windows [.] Net
- 9 oct 2018 godaddybeautifier270.blob.core.windows [.] Net
- 8 oct 2018 dropboxovertalkative.blob.core.windows [.] Net

La page de destination de phishing résultante est également un modèle relativement générique qui tente de tromper les victimes en leur demandant de donner leurs identifiants de messagerie Web pour le document promis relatif aux ouragans.

Figure 5: page de destination d'hameçonnage utilisant l'hébergement de blogs Microsoft Azure

Nous avons détecté plusieurs autres atterrissages liés à cette menace abusant de l'hébergement de blob bleu azur de Microsoft. Des exemples de ces pages qui abusent également d'autres marques fréquemment phishing apparaissent aux figures 6 à 9.

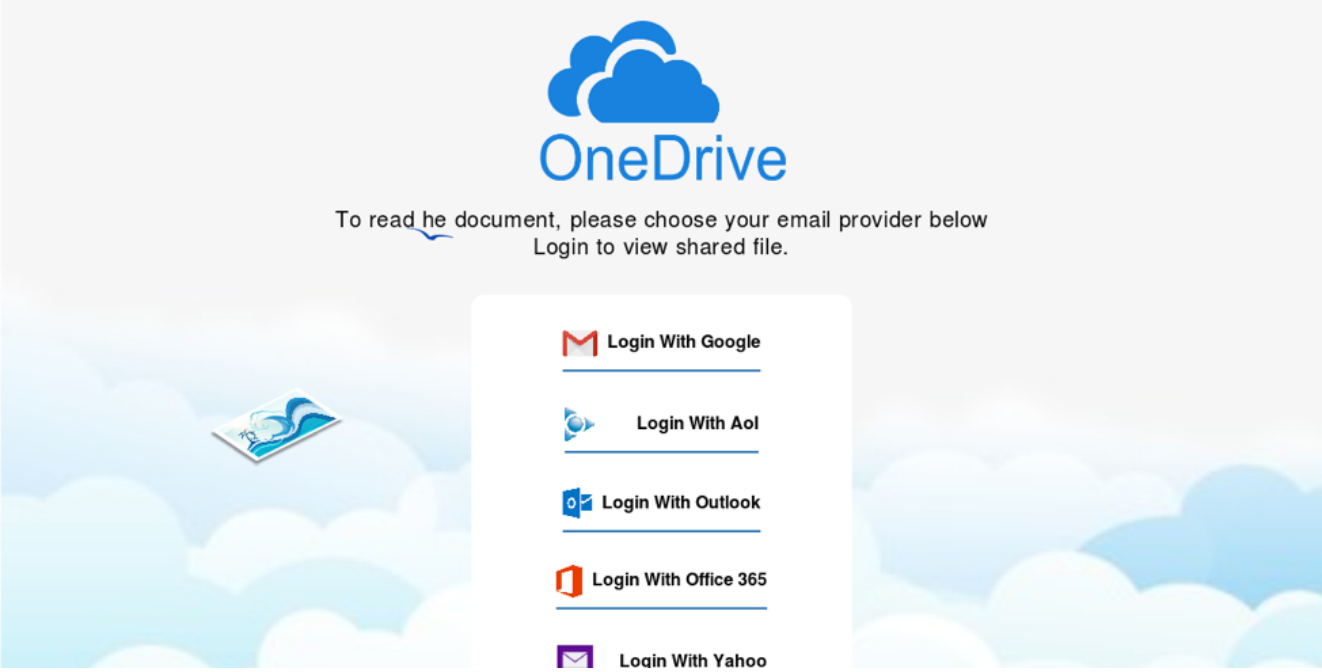

Figure 6: Une page de destination de phishing exploitant une infrastructure similaire et une image de marque volée pour le vol de justificatifs d'identité de messagerie

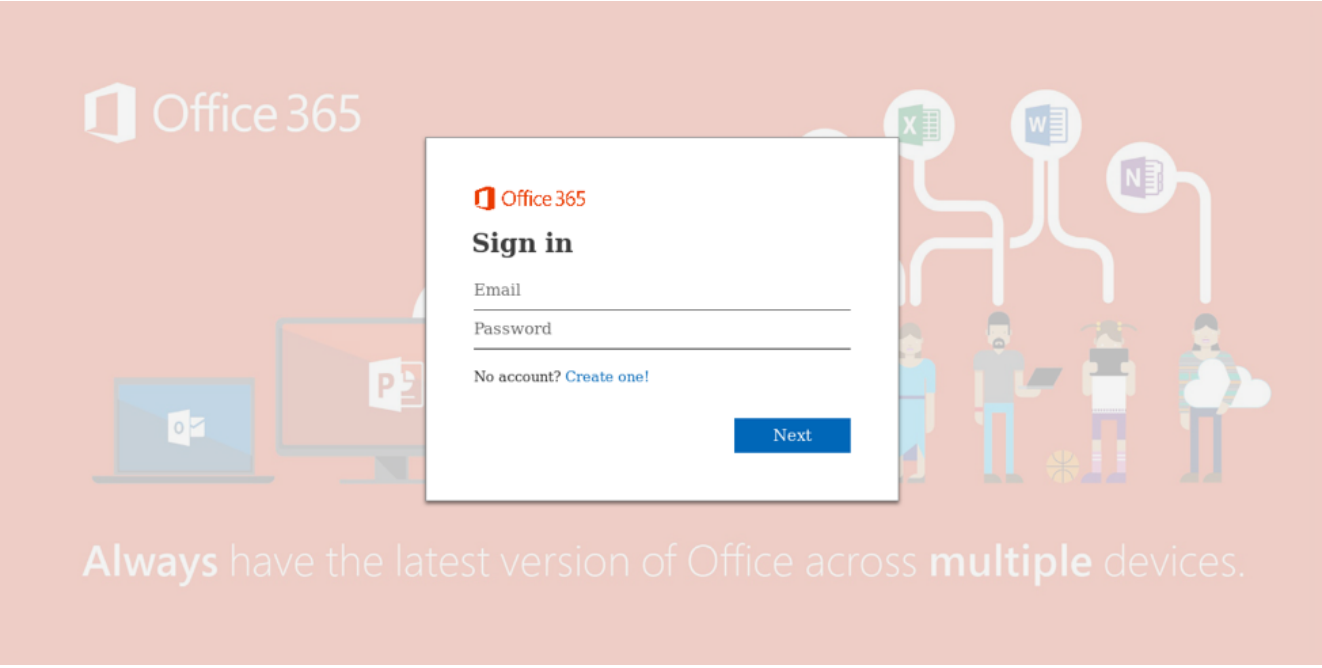

Figure 7: Une page de destination de phishing exploitant une infrastructure similaire et une image de marque volée pour le vol d'informations d'identification Microsoft Office 365

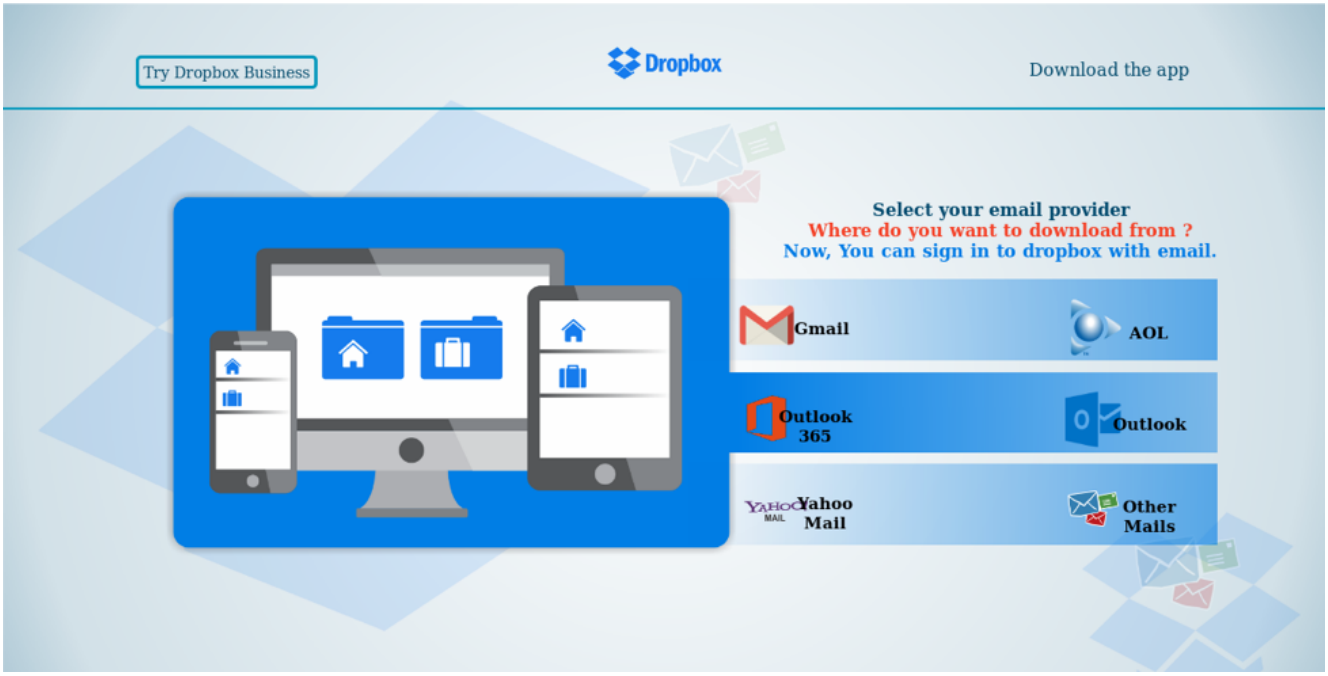

Figure 8: Une page de destination de phishing exploitant une infrastructure similaire et la marque Dropbox volée pour le vol de justificatifs d'identité de messagerie

Figure 9: Une page de destination de phishing exploitant une infrastructure similaire et l'image de marque Docusign volée pour le vol de justificatifs d'identité de messagerie

Conclusion

Les fraudes et les escroqueries apparaissent toujours autour d'événements majeurs, que ce soit les Jeux olympiques, les élections présidentielles ou les ouragans. Ces événements servent de leurres pour le phishing, les transactions frauduleuses et le vol direct.

Dans ce cas, les schémas de phishing se distinguent par le fait que les auteurs de la menace dirigent les destinataires vers des pages de vol de justificatif d'identité pour les courriers électroniques professionnels et personnels plutôt que pour le vol de carte de crédit ou financier.

Ceci est cohérent avec les augmentations spectaculaires que nous avons récemment observées dans le phishing par les entreprises. Toutefois, cela devrait également servir d'avertissement aux destinataires habitués à saisir les informations d'identification de messagerie pour se connecter à plusieurs services.

Les auteurs de la menace profitent à la fois de cette désensibilisation et de notre volonté de faire du bien. Bien qu'aucune d'entre elles ne soit une nouvelle tactique en soi, cette combinaison intéresse les défenseurs et les victimes potentielles. Ceux qui souhaitent faire des dons de bienfaisance ou demander de l'aide doivent se rendre directement sur les sites Web associés à des organisations de secours en cas de catastrophe connues et ne doivent jamais entrer de données d'identification de messagerie Web ou de médias sociaux pour permettre des dons.

[Note de la rédaction] Suite à nos sollicitations, Proofpoint assure ne disposer d'aucune donnée précise sur l'éventuelle exploitation des inondations de l'Aude pour mener des cyberattaques.