|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID du ticket** | **Message d'alerte** | **Gravité** | **Détails** | **Statut du ticket** |
| A-2703 | SERVEUR-E-MAIL Tentative d'hameçonnage, téléchargement possible d'un logiciel malveillant | Moyenne | L'utilisateur est susceptible d'avoir ouvert un e-mail malveillant ainsi que ses pièces jointes ou ses liens. | **Remonté** |

|  |
| --- |
| **Commentaires au sujet du ticket** |
| L'alerte a mis en évidence qu'un employé avait téléchargé et ouvert un fichier malveillant provenant d'un e-mail d'hameçonnage. Les informations suivantes sont incohérentes : l'adresse e-mail de l'expéditeur « 76tguy6hh6tgftrt7tg.su », le nom utilisé dans le corps de l'e-mail « Clyde West » et le nom de l'expéditeur, « Def Communications ». Des fautes de grammaire étaient présentes dans le corps et l'objet de l'e-mail. Le corps de l'e-mail contenait également une pièce jointe protégée par un mot de passe, intitulée « bfsvc.exe », qui a été téléchargée et ouverte sur l'appareil concerné. L'analyse du hachage du fichier a confirmé qu'il s'agit d'un fichier malveillant connu. D'autre part, la gravité de l'alerte est signalée comme moyenne. Compte tenu de ces constatations, j'ai décidé de transmettre ce ticket à un analyste SOC de niveau 2 afin qu'il prenne d'autres mesures. |

**Renseignements supplémentaires**

**Hachage du fichier malveillant connu** : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

**E-mail** :  
De : Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Date d'envoi : mercredi 20 juillet 2022 à 09:30:14

À : <hr@inergy.com> <176.157.125.93>  
Objet : Re : Poste d'inégiuer en infrastructure

Cher RH chez Ingergy,  
  
Je vous écris pour faire part de mon intérêt pour le poste d'ingénieur publié sur votre site web.  
  
Vous trouverez ci-joint mon CV et ma lettre de motivation. Pour des raisons de confidentialité, le fichier est protégé par un mot de passe. Utilisez le mot de passe « paradise10789 » pour l'ouvrir.   
  
Cordialement,  
  
Clyde West

Pièce jointe : filename="bfsvc.exe"