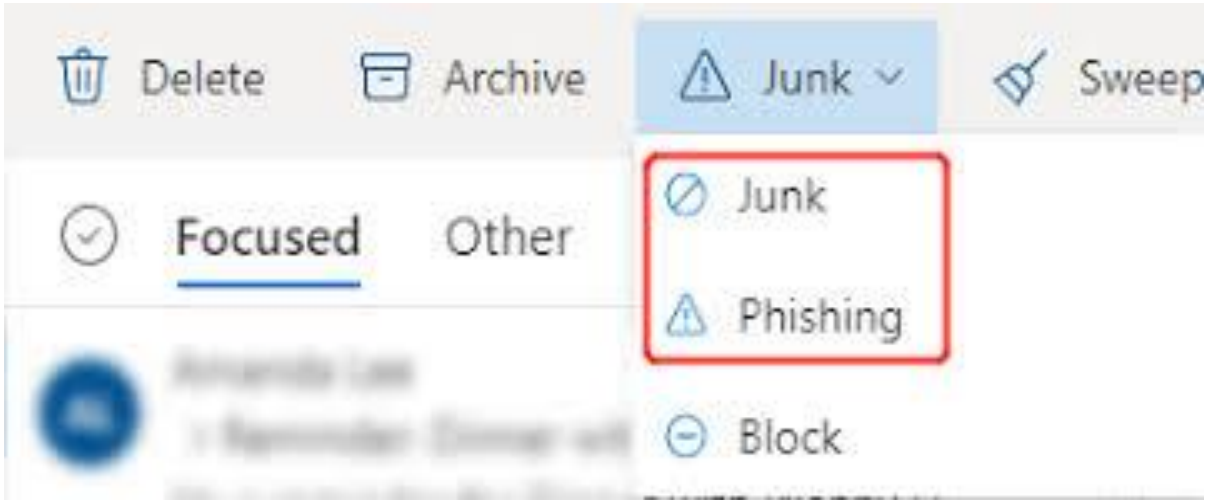
Oiseau Rouge

Fiche réflexe phishing

Récupération de mail de phishing

***Signalement utilisateur** : Signalement d'un mail suspect via des outils comme Outlook (bouton "Signaler un phishing") ou des systèmes internes (tickets, email dédié à la sécurité).*

***Plateformes d'analyse** : Les plateformes comme VirusTotal ou des outils internes pour collecter et analyser les informations.*



Oiseau Rouge

Analyse du mail signalé

Analyse visuelle du mail

1. **Objectifs d'un mail de phishing :**

- **Si le mail ne contient que du texte** :
  - *Obtenir des informations sensibles comme des identifiants (exemple : demande urgente de confirmation de compte bancaire).*
- **Si le mail contient une URL** :
  - *Rediriger vers un site frauduleux qui imite un site légitime pour voler des informations (exemple : pages de connexion pour des services comme PayPal, Amazon).*
- **Si le mail contient une pièce jointe** :
  - *Propager un logiciel malveillant (exemple : ransomware, keylogger) dès l'ouverture de la pièce jointe.*

2. **Comment les attaquants y parviennent :**

- **Utilisation de techniques de persuasion** :
  - *Création d'un sentiment d'urgence ou de peur (exemple : "Votre compte sera supprimé sous 24 heures si vous n'agissez pas").*
  - *Proposer une récompense attrayante (exemple : "Vous avez gagné un iPhone !").*
- **Usurpation d'identité** :
  - *Utilisation d'adresses email et de logos qui imitent ceux d'organisations fiables (exemple : banques, entreprises technologiques).*
- **Usage de liens ou pièces jointes malveillantes** :
  - *URL contenant des domaines ressemblants (exemple : "g0ogle.com" au lieu de "google.com").*
  - *Fichiers déguisés en PDF ou documents Word mais contenant des macros ou des exécutions malveillantes.*

3. **Différences entre un mail de spam et un mail de phishing :**

- **Mail de spam** :
  - *Contient souvent des publicités ou des offres commerciales non sollicitées.*

  - *L'objectif principal est promotionnel (exemple : vente de produits, services douteux).*
  - *Peu de risques directs pour la sécurité, mais peut être dérangeant.*
- **Mail de phishing** :
  - *Conçu pour tromper la victime et voler des données sensibles ou compromettre le système.*
  - *Cible des informations précises, comme les identifiants de connexion, les informations bancaires ou les données personnelles.*
  - *Souvent accompagné de menaces ou d'urgences pour forcer l'action rapide.*

Analyse des en-têtes du mail

Parties à regarder :

- ***From** : Vérifiez l'adresse email réelle de l'expéditeur.*
- ***Received** : Déterminez l'IP du serveur d'envoi.*
- ***Reply-To** : Vérifiez si elle diffère de l'expéditeur.*
- ***SPF/DKIM** : Vérifiez si le mail a passé ces protocoles pour détecter un spoofing.*

Analyse d'une URL

Comment analyser une URL :

- ***Vérifiez les anomalies** (domaines similaires mais différents comme "goog1e.com").*
- ***Utilisez des outils** comme VirusTotal, URLScan, ou PhishTank.*
- ***Ne cliquez jamais directement sur le lien.** Utilisez un navigateur sandboxé si nécessaire.*

Risques associés :

- ***Compromission des identifiants.***
- ***Téléchargement automatique d'un malware.***

Oiseau Rouge

Analyse d’une pièce jointe

Première analyse :

- *Vérifiez l’extension (exemple : .exe, .js, .bat, .docm).*
- *Scannez avec un antivirus ou un outil comme VirusTotal.*

Types de fichiers dangereux :

- *.exe, .js, .docm, .bat, .vbs.*

Quand escalader :

- *Si la pièce jointe est suspecte mais non détectée par les outils.*
- *Si elle est chiffrée ou protégée par mot de passe.*

Réponse et remédiation

Analyser l’impact d’une campagne de phishing

Analyser l’impact d’une campagne de phishing

- **Déterminer qui est touché :**
  - *Consultez les logs des emails pour identifier les destinataires.*
  - *Analysez qui a cliqué sur les liens ou ouvert les pièces jointes.*
- **À quel point un utilisateur peut être compromis :**
  - *Vérifiez les activités suspectes (connexions inhabituelles, changements de configuration).*
- ***Qui a accédé à des URL, des pièces jointes, etc. :***
- ***URL suspectes :***
  - *Consultez les **logs de proxy ou firewall** pour identifier les utilisateurs ayant tenté d'accéder à des URL malveillantes.*
  - *Recherchez les **blocs appliqués** par le système de sécurité.*
- ***Pièces jointes :***
  - *Vérifiez dans les **logs des solutions d’emailing** (Exchange, Microsoft 365 Defender) si une pièce jointe suspecte a été :*

Oiseau Rouge

        - *Ouverte par un utilisateur.*
        - *Signalée ou bloquée par un antivirus.*
- ***SIEM ou outils de monitoring :***
    - *Utilisez un SIEM (Splunk, QRadar, etc.) pour analyser les actions suivantes :*
        - ***Ouverture de fichiers suspects.***
        - ***Activité réseau anormale** après l'ouverture d'une pièce jointe ou d'un lien.*

Action à mener pour écarter la menace

Contacter :

- *L'utilisateur concerné pour lui faire changer son mot de passe et activer MFA.*
- *L'équipe IT pour bloquer l'expéditeur.*
- *Les équipes de sécurité pour analyser plus en détail.*

Prévention :

- *Former les utilisateurs sur le phishing.*
- *Mettre en place des filtres anti-phishing plus stricts.*

Liste de contacts d'urgence :

***◉ Équipe Sécurité (SOC) :** Responsable en charge des incidents de cybersécurité, contactable via security-team@entreprise.com.*

***◉ Support IT :** Service d'assistance technique pour bloquer les comptes compromis, disponible à it-support@entreprise.com ou au poste téléphonique interne.*

***◉ Référent Phishing :** Personne spécialisée dans l'analyse des attaques par phishing, joignable à phishing-report@entreprise.com.*

***◉ Responsable juridique :** Pour gérer les implications légales en cas de fuite de données, contact via legal@entreprise.com.*

***◉ CERT interne/externe :** Équipe de réponse aux incidents de sécurité (si applicable dans l'entreprise), contactable à cert@entreprise.com.*

Lorsque l'attaquant fait une demande au nom d'un autre utilisateur que le compte victime déjà en sa possession, au hasard un compte administrateur, le nom usurpé est disponible dans le champ... subject.Bingo !

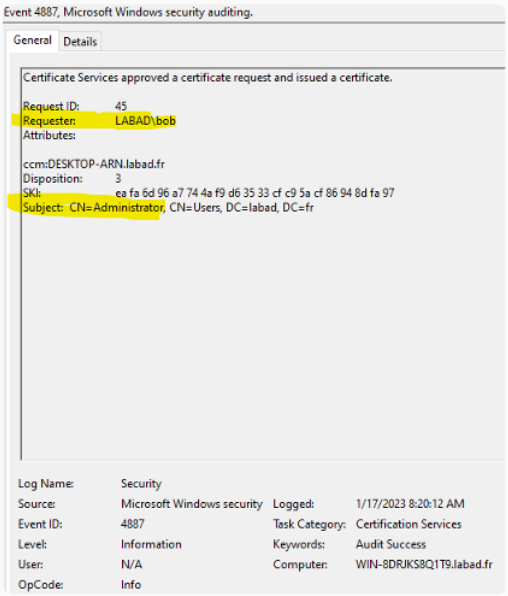


Figure 14. Aperçu d'un évènement Windows 4887

On voit dans l'image qu'on a bien une différence lors de l'approbation du certificat par la CA entre le champ « requester » et le « subject » avec le nom « Administrator » qui tente d'être usurpé.

Analyse de la capture :

- ***Contexte de compromission :***
  - *L'attaquant fait une demande au nom d'un autre utilisateur.*
  - *Le **champ "Requester"** montre l'utilisateur compromis.*
  - *Le **champ "Subject"** met en évidence l'usurpation avec le compte administrateur.*

- ***Informations clés dans la capture :***
  - ***Event ID 4887** : Un événement lié à la sécurité Windows (approbation d'un certificat).*
  - ***Nom du journal** : Sécurité (Security).*
  - ***Détails techniques** : Nom d'utilisateur usurpé, ordinateur, date et heure.*

- Phishing Email Analysis : 7 tips to identify it - SIEM XPERT

Oiseau Rouge

- Detecting Phishing Emails with Email Headers, Attachments, and URLs
- URL Analysis 101: A Beginner's Guide to Phishing URLs
- VirusTotal : analyser un fichier en ligne (virus, malware) – Le Crabe Info
  Sandboxing: Advanced Malware Analysis