PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 28/07/2025
N° CERTFR-2025-RFX-004

Compromission d'un tenant Azure - Endiguement

Fiche Réflexe

ANSSI/SDO
28/07/2025

Version : 1
Nombre de pages : 28

Table des matières

1 Présentation de la fiche **3**
- 1.1 À qui s'adresse-t-elle ? 3
- 1.2 Quand l'utiliser ? 3
- 1.3 À quoi sert-elle ? 3
- 1.4 Comment l'utiliser ? 3

2 Prérequis **4**
- 2.1 Avoir qualifié l'incident 4
- 2.2 Avoir les capacités d'administration 4
- 2.3 Ouvrir une main courante 5

3 Actions d'endiguement par priorités **5**
- 3.1 Cas 1 : Compromission d'un compte Microsoft 365 ou Microsoft Entra ID 7
- 3.2 Cas 2 : Compromission des identités d'applications dans Microsoft Entra 7
- 3.3 Cas 3 : Compromission d'application d'entreprise Microsoft Azure Entra 7
- 3.4 Cas 4 : Relai de contenu indésirable 7
- 3.5 Cas 5 : Fuite d'informations 7

4 Actions d'endiguement par cas **7**

5 Suite des actions **19**
- 5.1 Attaques considérées 20
- 5.2 Liens utiles 20
- 5.3 Définitions 22
- 5.4 Contacts 24
- 5.5 Déclarations 25
- 5.6 Préparation 25
- 5.7 Contacter le CERT-FR 26
- 5.8 Licence 27

1 Présentation de la fiche

1.1 À qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du tenant Azure

1.2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une compromission est suspectée ou confirmée au niveau d'un *tenant* Azure de l'organisation. Elle succède à l'étape de la fiche réflexe de qualification..

Utiliser cette fiche en cas de suspicion de compromission d'un *tenant* Azure, pouvant résulter de l'une des causes mentionnées ci-dessous :

- compromission de compte à privilèges Microsoft 365, notamment suite au vol de son mot de passe ;
- compromission de compte à privilèges Microsoft Entra ID, notamment suite au vol de son mot de passe ;
- compromission d'application, ou caractère malveillant d'application d'entreprise intégrée à Microsoft Entra ID ;
- altération malveillante de la configuration sécurité du *tenant* Microsoft 365 ;
- altération malveillante de la configuration sécurité du *tenant* Microsoft Entra ;
- compromission de compte utilisateur Microsoft 365 / Entra ID.

1.3 À quoi sert-elle ?

L'objectif de cette fiche n'est pas de proposer les premières actions d'*endiguement* ayant pour objectif de circonscrire l'attaque. Elles tenteront de *limiter son extension et son impact* et de donner du temps aux défenseurs pour s'organiser et reprendre l'initiative.

Cette fiche ne prétend pas couvrir l'ensemble des attaques possibles sur Microsoft 365 et Entra ID, mais se concentre sur celles fréquemment rencontrées lors des réponses à incidents, à savoir :

1.4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

CC BY-NC-SA 4.0

- La partie Actions d'endiguement par priorités pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante.

- La partie Actions d'endiguement par cas détaille les différentes actions d'endiguement possibles selon les cas de compromission.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie Contacts.

2 Prérequis

Note

En cas de suspicion de compromission de poste de travail intégré à Entra ID ou de machine virtuelle hébergée sur la plateforme Microsoft Azure, il est recommandé de se référer à la fiche réflexe de compromission d'un système. Si un compte Microsoft Entra ID a été utilisé sur le poste de travail pré-compromission supposée, alors il est recommandé de dérouler également la présente fiche réflexe.

2.1 Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur le système d'information soit bien une compromission de tenant [1] Azure, et en avoir évalué la gravité :

Fiche précédente conseillée : Fiche réflexe - Compromission d'un tenant Azure - Qualification

Les mesures d'endiguement proposées dans cette fiche devront être appliquées en cohérence avec les conclusions de la *qualification* : le *périmètre* affecté par l'incident, son *impact* potentiel sur l'organisation, l'*urgence* à résoudre la situation, etc.

2.2 Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les *droits d'administration* du tenant Azure.

Dans le cas où l'attaque aurait compromis un compte d'administration, il est essentiel de disposer d'un autre compte doté de privilèges d'administration suffisamment élevés (idéalement équivalents à ceux d'un compte Administrateur général).

1. Le terme de *tenant* (ou *locataire*) Azure désigne souvent ce même environnement au niveau des services Microsoft 365, et/ou Entra ID (anciennement Azure AD).

CC BY-NC-SA 4.0

Si le système d'information est *infogéré*, s'assurer de la capacité à mobiliser leur support technique dans l'urgence.

2.3 Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer tous les actions et évènements survenus sur le système d'information dans un *ordre chronologique*.

Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La **date et l'heure** de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC)
2. Le **nom de la personne** en charge de cette action ou ayant informé sur l'évènement (ou le nom du service de sécurité ayant détecté l'évènement).
3. La **description** de l'action ou de l'évènement, incluant les détails de son avancement ainsi que les comptes et machines concernés.

Ce document sera utile pour :

- Réaliser un historique du traitement de l'incident et partager la connaissance
- Piloter la coordination des actions et suivre leur état d'avancement
- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus

Cette main courante doit être éditable et consultable par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident ou le SIEM si l'organisation en possède un, voire être au format papier.

3 Actions d'endiguement par priorités

Cette section présente l'ordre chronologique et prioritaire des actions, qui seront détaillées dans la partie suivante. Plusieurs scénarios peuvent se présenter, chacun nécessitant des actions spécifiques :

CC BY-NC-SA 4.0

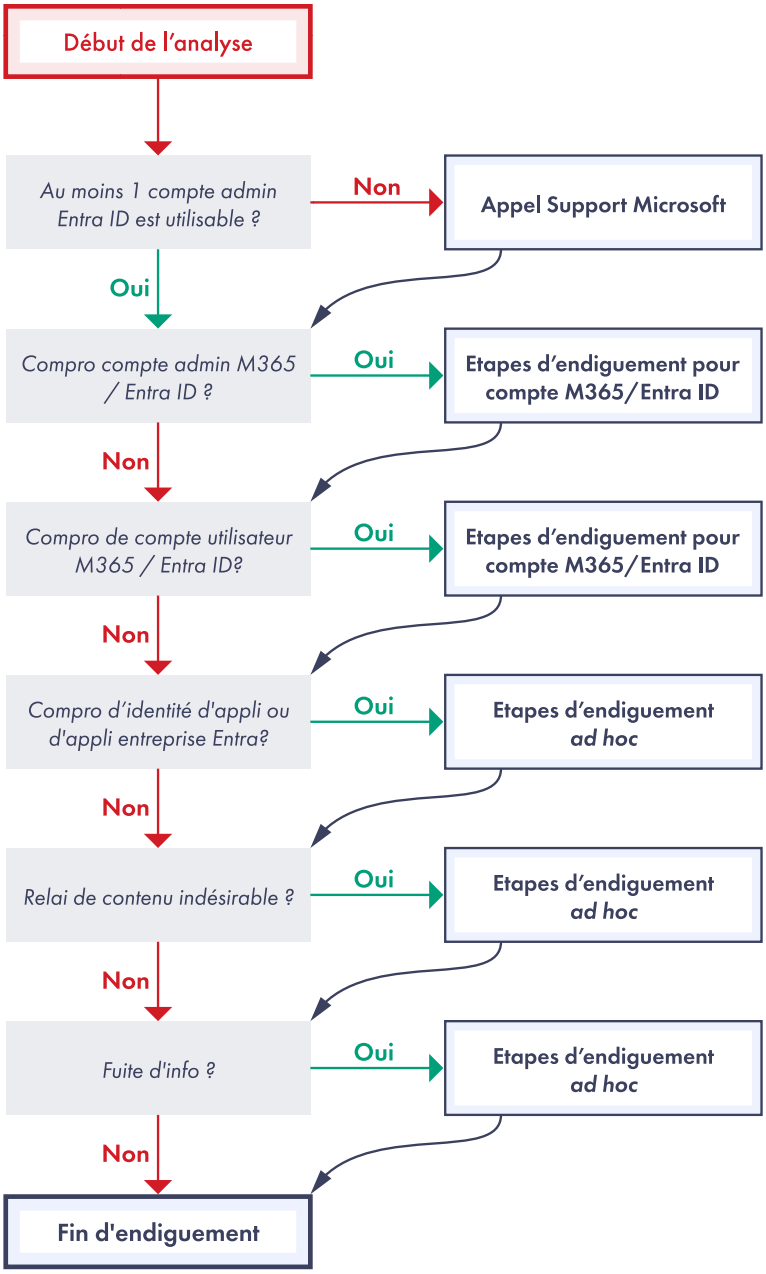


FIGURE 1 – Etapes de l'endiguement

CC BY-NC-SA 4.0

3.1 Cas 1 : Compromission d'un compte Microsoft 365 ou Microsoft Entra ID

Actions	Priorité
Réinitialiser le mot de passe des comptes compromis (Action 1.a)	P0
Révoquer les sessions actives (Action 1.b)	P0
Désactiver le compte (Action 1.c)	P0
Exiger une réinscription de l'authentification multifacteur (Action 1.d)	P0
Durcir la stratégie d'accès conditionnel (Action 1.e)	P1
Révoquer les rôles attribués illégitimes (Action 1.f)	P1

3.2 Cas 2 : Compromission des identités d'applications dans Microsoft Entra

Actions	Priorité
Désactiver la connexion vers l'application compromise ou malveillante (Action 2.a)	P0
Réviser les accès et permissions de l'application compromise (Action 2.b)	P0
Réinitialiser les certificats et secrets compromis de l'application (Action 2.c)	P0
Supprimer tous les rôles Entra illégitimes attribués à l'application compromise (Action 2.d)	P0
Supprimer ou restaurer la configuration des rôles et administrateurs pour l'application compromise (Action 2.e)	P0
Restaurer explicitement le propriétaire légitime de l'application compromise (Action 2.f)	P1
Rendre obligatoire le consentement explicite d'un administrateur pour toute nouvelle application tierce (Action 2.g)	P1

3.3 Cas 3 : Compromission d'application d'entreprise Microsoft Azure Entra

Actions	Priorité
Isoler les ressources compromises par l'attaquant (Action 3.a)	P0
Révoquer les identifiants potentiellement compromis présents sur la ressource (Action 3.b)	P0

3.4 Cas 4 : Relai de contenu indésirable

Actions	Priorité
Restaurer la configuration anti-spam compromise (Action 4.a)	P0
Restaurer la politique anti-spoofing compromise (Action 4.b)	P0
Renforcer la configuration anti-spam pour éviter une récidive (Action 4.c)	P1

3.5 Cas 5 : Fuite d'informations

Actions	Priorité
Supprimer les règles de transfert illégitimes (Action 5.a)	P0
Supprimer les règles de transport illégitimes (Action 5.b)	P0
Désactiver l'authentification directe sur les boîtes aux lettres partagées (Action 5.c)	P0
Désactiver les protocoles historiques (IMAP, POP, SMTP Auth) (Action 5.d)	P0
Supprimer les extensions de pièces jointes non autorisées (Action 5.e)	P0
Supprimer les délégations illégitimes d'une boîte de messagerie (Action 5.f)	P0

4 Actions d'endiguement par cas

Cette partie détaille les différentes mesures d'endiguement possibles selon les cas de compromission de l'environnement Azure. Chaque cas est ensuite scindée en actions unitaires :

CC BY-NC-SA 4.0

4.0.1 Cas 1 : Compromission d'un compte Microsoft 365 ou Entra ID

Action 1.a : Réinitialiser le mot de passe du compte compromis

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Utilisateurs" > "Utilisateurs actifs"
- ☐ Sélectionner le nom de l'utilisateur, puis sélectionner "Réinitialiser le mot de passe"
- ☐ Sélectionner "Réinitialiser le mot de passe" une seconde fois pour obtenir le mot de passe temporaire

Action 1.b : Révoquer les sessions actives

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Utilisateurs" > "Utilisateurs actifs"
- ☐ Sélectionner le nom de l'utilisateur, puis "Révoquer les sessions"

Action 1.c : Désactiver le compte

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Utilisateurs" > "Utilisateurs actifs"
- ☐ Sélectionner le nom de l'utilisateur, puis "Modifier les propriétés", aller sur l'onglet "Paramètres"
- ☐ Décocher "Compte activé", sélectionner "Enregistrer"

Action 1.d : Exiger une réinscription de l'authentification multifacteur

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Utilisateurs" > "Utilisateurs actifs"
- ☐ Sélectionner le nom de l'utilisateur, puis "Méthodes d'authentification"
- ☐ Sélectionner "Exiger une réinscription de l'authentification multifacteur", puis "Ok"

CC BY-NC-SA 4.0

Action 1.e : Durcir la stratégie d'accès conditionnelle

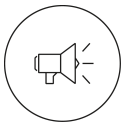
- ☐ Bloquer des adresses IP sources ayant un comportement qualifié de malveillant et filtrage géographique
  - ☐ Se connecter à `https://entra.microsoft.com`
  - ☐ Aller sur la page "Protection" > "Accès conditionnel"
  - ☐ Créer la stratégie d'accès conditionnelle

Action 1.f : Révoquer les rôles Entra ID illégitimes

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Utilisateurs" > "Utilisateurs actifs"
- ☐ Sélectionner le nom du compte, puis "Rôles affectés"
- ☐ Supprimer les rôles illégitimes du compte

Action 5.a : Supprimer les règles de transfert illégitimes

- ☐ Voir l'action 5.a du Cas 5



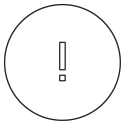
Remarque

- S'assurer de disposer d'au moins deux comptes de confiance avec le rôle "Administrateur général" du *tenant* avant de poursuivre
- Réduiser au minimum absolu le nombre de comptes avec des rôles d'administration privilégiés
- Faites régulièrement des revues d'accès pour valider que chaque utilisateur a encore besoin des rôles sensibles
- Envisager l'utilisation de Microsoft Entra ID pour surveiller les utilisateurs privilégiés et détecter des connexions inhabituelles
- S'assurer que la politique des mots de passe est conforme aux exigences de complexité (vérifier sa politique de mot de passe)

4.0.2 Cas 2 : Compromission d'application d'entreprise Microsoft Azure Entra

CC BY-NC-SA 4.0

Action 2.a : Désactiver la connexion vers l'application compromise ou malveillante



Important

Avant de désactiver une application, évaluer soigneusement l'impact sur les activités métiers par rapport au risque de sécurité. Si l'impact est trop élevé, préparez-vous à passer directement à l'étape "Action 2.b".

☐ Se connecter à `https://entra.microsoft.com`

☐ Aller sur la page "Applications" ← "Applications d'entreprise"

  ☐ Sélectionner l'application compromise (supprimer les filtres si nécessaire), puis aller dans "Propriétés"

☐ Désactiver l'application en définissant "Activée pour la connexion des utilisateurs ?" sur « Non »
Aucun jeton ne sera délivré à l'application, qui ne pourra donc plus appeler Microsoft Graph ni aucune autre API protégée par Microsoft Entra. Cela permettra de conserver les paramètres de configuration avant la suppression de l'application, facilitant ainsi les investigations.

- Dans le cas d'une application malveillante
  - À la fin des investigations, supprimer les applications malveillantes
- Dans le cas d'applications compromises
  Il est préférable de créer et de configurer une nouvelle application, afin de s'assurer qu'aucun paramètre oublié ne puisse rétablir un accès malveillant.
  - À la fin des investigations ,supprimer les applications compromises désactivées

☐ Explorer d'autres options pour renforcer la sécurité des applications :

- Accès conditionnel pour les identités de service
- Politiques de risque applicatif

Action 2.b : Révision des accès d'une application compromise qui n'est pas désactivée en raison de l'impact potentiel

☐ Se connecter à `https://entra.microsoft.com`

☐ Aller sur la page "Applications" > "Applications d'entreprise"

CC BY-NC-SA 4.0

☐ Sélectionner l'application compromise (supprimer les filtres si nécessaire), puis aller dans "Autorisations"

☐ Sélectionner l'option "Révision des autorisations"

☐ Sélectionner l'option "Cette application est malveillante et je suis compromis." :

- Utiliser les trois scripts Powershell proposés pour nettoyer rapidement la configuration de l'authentification de l'application
  L'installation du module Powershell "Microsoft.Graph" est un prérequis et s'installe à l'aide de la commande suivante :

  ```
  Install-Module Microsoft.Graph -Scope CurrentUser
  ```

  Les scripts Powershell permettent de :

  1. Supprimer tous les utilisateurs affectés pour les empêcher de se connecter à l'application.
  2. Invalider les jetons d'actualisation pour les utilisateurs qui ont accès à l'application.
  3. Révoquer toutes les autorisations pour cette application.

- Dans Propriétés, exiger l'affectation d'un utilisateur pour accéder à l'application.

- Dans Autorisations, vérifier les consentements accordés à cette application :
  - Dans "Consentement d'administrateur", révoquer les autorisations illégitimes.
  - Dans "Consentement d'utilisateur", révoquer les autorisations illégitimes.

- Dans Utilisateurs et groupes, vérifier les utilisateurs affectés à cette application :
  - Supprimer les utilisateurs illégitimes affectés à l'application.

Action 2.c : Réinitialiser les certificats et secrets d'une application compromise qui n'est pas désactivée

☐ Se connecter à `https://entra.microsoft.com`
☐ Aller sur la page "Applications" > "Inscriptions d'applications" > "Certificats & Secret"
Les certificats ou secrets peuvent avoir été configurés ou compromis par l'attaquant

☐ Supprimer les certificats et les secrets

☐ Recréer des certificats et des secrets légitimes si nécessaire

CC BY-NC-SA 4.0

Action 2.d : Supprimer tous les rôles Entra illégitimes d'une application compromise qui n'est pas désactivée

- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Rôles et administrateurs"
- ☐ Sélectionner "Télécharger les attributions", puis une fois le fichier généré ,cliquer sur "Le fichier est prêt ! Cliquez ici pour télécharger"
  Une recherche depuis le fichier va permettre d'identifier les rôles illégitimes associés aux applications plus rapidement
  - ☐ Sélectionner les rôles illégitimes puis retirer les applications membres compromises

Action 2.e : Supprimer ou restaurer la configuration des "Rôles et administrateurs" utilisée pour l'administration d'une application compromise qui n'est pas désactivée

- ☐ Identifier toute modification récente suspecte apportée aux rôles administratifs des applications
- ☐ Se connecter à `https://entra.microsoft.com`
- ☐ Aller sur la page "Applications" > "Applications d'entreprise" ← "Rôles et administrateurs"
- ☐ Restaurer ou remettre en place la configuration des rôles et administrateurs légitimes initiaux

Action 2.f : Restaurer explicitement le propriétaire d'une application compromise qui n'est pas désactivée

- ☐ Identifier les applications dont les propriétaires et administrateurs ont été modifiés illégalement
- ☐ Se connecter à `https://entra.microsoft.com` ← Applications ← Inscriptions d'applications ← Sélectionner l'application concernée
- ☐ Modifier l'attribution du propriétaire pour rétablir l'administrateur ou l'équipe applicative légitime
- ☐ Informer immédiatement le propriétaire rétabli et lui demander de vérifier les permissions et configurations sensibles de son application

Action 2.g : Rendre obligatoire le consentement explicite d'un administrateur pour toute nouvelle application tierce

- ☐ Limiter l'accord aux utilisateurs pour l'inscription d'applications ayant un « impact faible » comme pour les applications provenant d'éditeurs vérifiés, ou pour les applications

CC BY-NC-SA 4.0

enregistrées dans cette organisation.

☐ Se connecter à `https://entra.microsoft.com`

☐ Aller sur la page "Applications" ← "Applications d'entreprise" > "Consentement et autorisations" > "Paramètres de consentement de l'utilisateur"

☐ Sélectionner "Autoriser le consentement de l'utilisateur pour les applications provenant d'éditeurs vérifiés, pour les autorisations sélectionnées"

☐ Cliquer sur "Enregistrer"

☐ Aller sur l'onglet "Paramètres du consentement de l'administrateur"

☐ Activer "Les utilisateurs peuvent demander le consentement d'administrateur pour les applications qu'ils ne peuvent pas accepter" sur "Oui"

☐ Configurer les utilisateurs, groupes ou rôles qui peuvent réviser les demandes de consentement de l'administrateur

☐ Cliquer sur "Enregistrer"

4.0.3 Cas 3 : Compromission d'une ressource Azure

Action 3.a : Isoler les ressources Azure compromises par l'attaquant

Procéder à l'isolation des ressources concernées selon leur type :

☐ **Machine virtuelle (VM)** :

- Déconnecter l'interface réseau (NIC) ou appliquer un groupe de sécurité réseau (NSG) très restrictif
- Mettre en pause la VM pour stopper l'activité malveillante est aussi une solution

☐ **Ressource PaaS (App Service, Azure Function)** :

- Désactiver temporairement le service via le portail Azure (mettre à l'arrêt l'App Service ou la Function)
- Bloquer l'accès externe via modification des règles réseau (restriction d'accès IP)

☐ **Compte de stockage Azure (Storage Account)** :

- Désactiver tout accès public ou générer de nouvelles clés d'accès (storage keys)

CC BY-NC-SA 4.0

- Restreindre l'accès via Firewall intégré au compte de stockage

☐ Confirmer la réussite de l'isolation en validant l'absence de nouvelles alertes après l'opération :

- trafic entrant ou sortant malveillant
- alertes antivirus/EDR
- Microsoft Defender for Cloud,
- etc.

Action 3.b : Révoquer les identifiants potentiellement compromis présents sur la ressource Azure

☐ Révoquer et renouveler les identifiants compromis ou à risque :

- Renouveler les clés d'accès ou secrets d'Azure Key Vault utilisés par la ressource
- Renouveler les tokens d'accès aux API ou services externes que la ressource utilise
- Modifier les mots de passe des comptes techniques locaux utilisés par la ressource (ex : comptes locaux sur une VM)

☐ Mettre à jour les configurations applicatives concernées pour qu'elles utilisent les nouveaux identifiants sécurisés
☐ Confirmer que les anciens identifiants compromis ne peuvent plus être utilisés (vérification pratique ou audit des accès tentés après révocation)

4.0.4 Cas 4 : Relai de contenu indésirable

Action 4.a : Restaurer la configuration anti-spam compromise

☐ Se connecter à `https://security.microsoft.com/tenantAllowBlockList`

☐ Supprimer les domaines et adresses illégitimes

Action 4.b : Renforcer la configuration anti-spam pour éviter une récidive

☐ Appliquer une politique plus stricte pour les utilisateurs à risque (VIP, comptes techniques, direction)

☐ Se connecter à `https://security.microsoft.com/presetSecurityPolicies`

☐ Créer une stratégie pour "Protection stricte"

CC BY-NC-SA 4.0

☐ Activer la quarantaine systématique pour les emails suspects

☐ Se connecter à https://security.microsoft.com/antispam

☐ Activer les notifications d'administrateur pour les envois ou réceptions massifs

Action 4.c : Restaurer la politique anti-spoofing compromise

☐ Se connecter à https://security.microsoft.com/antiphishing

☐ Vérifier les paramètres de la stratégie anti-hameçonnage dans Microsoft 365 Defender

☐ Sélectionner la règle activée

☐ Réviser les entrées de type :

- expéditeurs
- domaine(s) personnalisé(s)
- expéditeur(s) et domaine(s) approuvé(s)

4.0.5 Cas 5 : Fuite d'informations

Action 5.a : Supprimer les règles de transfert illégitimes

☐ Ouvrir une console Powershell
L'installation du module Powershell "ExchangeOnlineManagement" est un prérequis et s'installe à l'aide de la commande suivante.

```
Install-Module ExchangeOnlineManagement `
    -Scope CurrentUser
```

☐ Se connecter à Exchange Online PowerShell :
Remplacer <admin@votredomaine.com> par l'adresse e-mail du compte administrateur Exchange Online.

```
Connect-ExchangeOnline `
    -UserPrincipalName <admin@votredomaine.com> `
    -ShowProgress $true
```

☐ Lister les règles de boîte de réception d'un utilisateur :
Remplacer `<utilisateur@votredomaine.com>` par l'adresse e-mail de l'utilisateur dont vous souhaitez consulter les règles.

```
Get-InboxRule `
    -Mailbox "<utilisateur@votredomaine.com>"
```

☐ Supprimer les règles illégitimes :
Remplacer `<NomDeLaRègle>` par le nom exact de la règle à supprimer.

```
Remove-InboxRule `
    -Mailbox "<utilisateur@votredomaine.com>" `
    -Identity "<NomDeLaRègle>"
```

Action 5.b : Supprimer les règles de transport illégitimes

☐ Se connecter à `https://admin.exchange.microsoft.com/#/transportrules`

☐ Identifier toute règle suspecte (ex : redirection vers une adresse externe, copie cachée)

☐ Désactiver ou supprimer les règles illégitimes

☐ Restaurer une configuration saine si un export de règles existe

Action 5.c : Désactiver l'authentification directe sur les boîtes aux lettres partagées (via IMAP, POP, SMTP Auth, MAPI, OWA)

☐ Identifier toutes les boîtes aux lettres partagées avec une authentification directe activée

☐ Ouvrir une console Powershell
L'installation du module Powershell "ExchangeOnlineManagement" est un prérequis et s'installe à l'aide de la commande suivante :

```
Install-Module ExchangeOnlineManagement `
    -Scope CurrentUser
```

☐ Lister les boîtes aux lettres partagées avec une authentification directe activée :

CC BY-NC-SA 4.0

```
Get-Mailbox -RecipientTypeDetails SharedMailbox `
    | Get-CASMailbox
```

☐ Désactiver les accès directs (IMAP, POP, MAPI, OWA) si activés
Remplacer <BAL> par l'adresse email de la boîte de messagerie.

```
Set-CASMailbox `
    -Identity "<BAL>" `
    -MAPIEnabled $false
```

☐ Conserver uniquement l'accès via délégation sur un compte utilisateur authentifié

Action 5.d : Désactiver les protocoles historiques (IMAP, POP, SMTP Auth)

☐ Ouvrir une console Powershell
L'installation du module Powershell "ExchangeOnlineManagement" est un prérequis et s'installe à l'aide de la commande suivante :

```
Install-Module ExchangeOnlineManagement `
    -Scope CurrentUser
```

☐ Vérifier les protocoles autorisés au niveau du tenant et par utilisateur

```
Get-CASMailbox `
    | Where-Object {$_.PopEnabled -eq $true -or $_.ImapEnabled -eq $true}
```

☐ Désactiver les protocoles obsolètes sauf nécessité métier justifiée Remplacer <utilisateur> par l'adresse email de la boîte de messagerie.

```
Set-CASMailbox `
    -Identity "<utilisateur>" `
    -PopEnabled $false `
    -ImapEnabled $false `
    -SmtpClientAuthenticationDisabled $true
```

☐ Surveiller si certains comptes tentent encore d'utiliser ces protocoles (alerte Defender)

CC BY-NC-SA 4.0

Action 5.e : Supprimer les extensions de pièces jointes non autorisées

☐ Ouvrir une console Powershell. L'installation du module Powershell "ExchangeOnlineManagement" est un prérequis et s'installe à l'aide de la commande suivante :

```
Install-Module ExchangeOnlineManagement `
    -Scope CurrentUser
```

☐ Se connecter à Exchange Online PowerShell. Remplacer `<admin@votredomaine.com>` par l'adresse e-mail du compte administrateur Exchange Online.

```
Connect-ExchangeOnline `
    -UserPrincipalName <admin@votredomaine.com> `
    -ShowProgress $true
```

☐ Modifier les politiques anti-malware d'Exchange Online. Interdire l'envoi/réception de fichiers par exemple `.exe`, `.js`, `.vbs`, `.scr`, etc.
Remplacer `<"exe", "js", "vbs", "scr">` par les extensions souhaitées.

```
New-TransportRule `
    -Name "Bloquer les pièces jointes exécutables" `
    -AttachmentExtensionMatchesWords <"exe", "js", "vbs", "scr"> `
    -RejectMessageReasonText `
        "Les fichiers exécutables sont bloqués pour des raisons de sécurité." `
    -Enabled $true
```

☐ Ajouter des règles supplémentaires pour bloquer des extensions spécifiques utilisées lors de l'incident (si connues)
☐ Définir et surveiller les alertes, car elles pourront permettre d'identifier un compte compromis non encore identifié

Action 5.f : Supprimer les délégations illégitimes d'une boîte de messagerie

☐ Se connecter à `https://admin.cloud.microsoft/exchange#/mailboxes`

☐ Sélectionner le compte de boîte de messagerie

☐ Supprimer les délégations illégitimes de la boîte de messagerie pour les trois types :

CC BY-NC-SA 4.0

- Envoyer en tant que
- Envoyer de la part de
- Lecture et gestion (accès total)

☐ Se connecter à Exchange Online PowerShell.
Remplacer `<admin@votredomaine.com>` par l'adresse e-mail du compte administrateur Exchange Online.

```
Connect-ExchangeOnline `
    -UserPrincipalName <admin@votredomaine.com>`
    -ShowProgress $true
```

☐ Modifier les politiques anti-malware d'Exchange Online. Interdire l'envoi/réception de fichiers par exemple `.exe`, `.js`, `.vbs`, `.scr`, etc. Remplacer `<"exe", "js", "vbs", "scr">` par les extensions souhaitées.

```
New-TransportRule `
    -Name "Bloquer les pièces jointes exécutables"  `
    -AttachmentExtensionMatchesWords <"exe", "js", "vbs", "scr"> `
    -RejectMessageReasonText `
        "Les fichiers exécutables sont bloqués pour des raisons de sécurité." `
    -Enabled $true
```

☐ Ajouter des règles supplémentaires pour bloquer des extensions spécifiques utilisées lors de l'incident (si connues)

5 Suite des actions

À la fin de ces actions d'endiguement, la compromission devrait être contenue au sein du tenant Azure. Pour autant, l'incident a très probablement impacté l'organisation au-delà de son environnement cloud et il reste encore beaucoup à faire.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : investigation forensique et remédiation par une équipe spécialisée, maintien d'activité, communication interne aux partenaires, dépôt de plainte et déclarations, etc.

Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident accompagné par un CERT en cohérence avec les impacts identifiés :

CC BY-NC-SA 4.0

- Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident
  - Voir les annexes **Contacts** et **Déclarations**
- De plus, si l'incident a un **périmètre étendu** sur le système d'information, qu'il a un **impact fort** et qu'il nécessite une **résolution urgente** :
  - Activer le dispositif de **gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité
  - Guide conseillé : Crise cyber, les clés d'une gestion opérationnelle et stratégique.

5.1 Attaques considérées

Type d'attaque	Référence MITRE ATT&CK
Business Email Compromise (BEC) et *Email Account Compromise* (EAC)[2],	BEC : T1586.002, EAC : T1078.004
Fuite d'information : exfiltration d'emails , partage de fichiers, accès illégitime à des espaces Teams…	T1114, T1213
Utilisation illégitime d'un compte utilisateur (à privilèges ou non) Microsoft 365	T1078.004
Rebond, avec diffusion de contenus malveillants depuis le *tenant* Microsoft 365, ex. : courriels indésirables tels que du spam et hameçonnage	T1496.004
Application d'entreprise Microsoft Entra légitime vulnérable exploitée	T1190 et/ou T1528
Application d'entreprise Microsoft Entra malveillante installée par un utilisateur	T1496.004 notamment

Note

Par extension, il est également possible de qualifier certains cas d'attaque de type diffusion de fichier malveillant hébergé sur un lien OneDrive/SharePoint/Teams du *tenant* investigué (MITRE ATT&CK T1021.007).

Les différentes actions proposées aideront à :

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'il peut être considéré comme une compromission, totale ou partielle, du *tenant* Microsoft 365 ou Entra ID ;
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

Pour de plus amples détails sur les types d'attaques pouvant cibler Microsoft 365 et Entra ID (anciennement Azure AD), il est conseillé de se référer à la section liens utiles en fin de cette fiche.

5.2 Liens utiles

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

2. cf. section liens utiles pour plus d'informations sur l'attaque dite du BEC

CC BY-NC-SA 4.0

5.2.1 Guides

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
  https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber
- Fiche réflexe - Compromission d'un tenant Azure - Qualification

5.2.2 Présentation de concepts

- Qu'est-ce que les services Microsoft 365 ?
  https://learn.microsoft.com/fr-fr/office365/servicedescriptions/office-365-service-descriptions-technet-library
- Qu'est-ce que Microsoft Entra et les identifiants Entra ID ?
  https://learn.microsoft.com/fr-fr/entra/fundamentals/whatis
- Applications Microsoft Entra
  https://learn.microsoft.com/fr-fr/entra/identity/enterprise-apps/what-is-application-management
- Rôles Microsoft Entra
  https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference
- Rôles Microsoft 365
  https://learn.microsoft.com/fr-fr/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide
- Règles de transport Exchange Online
  https://learn.microsoft.com/fr-fr/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
- "RemoteDomain" dans Exchange Online
  https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/remote-domains/remote-domains
- Fédération Microsoft Entra ID entre organisations
  https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/whatis-fed
- Présentation rapide de Microsoft Graph
  https://learn.microsoft.com/fr-fr/graph/overview

5.2.3 Recommandations

- 10 principales façons de sécuriser Microsoft 365 et Entra ID, selon le niveau de licence
  https://learn.microsoft.com/fr-fr/microsoft-365/business-premium/secure-your-business-data?view=o365-worldwide
- Recommandation de sécurisation des BAL partagées, niveau authentification
  https://www.tenable.com/audits/items/CIS_Microsoft_365_v3.1.0_E3_Level_1.audit:cfcd96ef3d222577b0aef7c8d2fc4ad3
- Recommandations Microsoft pour la remédiation d'attaques utilisant les règles Outlook
  https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

CC BY-NC-SA 4.0

- Recommandations Microsoft pour la détection et le traitement de l'attaque "Illicit consent Grant"
  https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants?view=o365-worldwide#what-is-the-illicit-consent-grant-attack-in-microsoft-365
- Empêcher un ancien employé de se connecter et bloquer l'accès aux services Microsoft 365
  https://learn.microsoft.com/fr-fr/microsoft-365/admin/add-users/remove-former-employee-step-1?view=o365-worldwide#block-a-former-employees-access-to-email-exchange-online
- Recommandations Microsoft pour l'attaque de pulvérisation de mots de passe
  https://learn.microsoft.com/fr-fr/security/operations/incident-response-playbook-password-spray
- Dlux de travaux recommandé par Microsoft pour cas d'usage de compromission d'application Azure
  https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-compromised-malicious-app

5.2.4 Attaques

- Attaque dite "Business Email Compromise"
  https://www.microsoft.com/fr-fr/security/business/security-101/what-is-business-email-compromise-bec
- Common attacks targeting Microsoft 365 and Azure AD
  https://blog.microwavewitness.eu/work/microsoft/m365_attacks/
- Abusing Azure application credentials to attack supply chains
  https://www.secureworks.com/research/abusing-azure-application-credentials-to-attack-supply-chains
- Matrice ATT&CK pour les services Office de type Microsoft 365
  https://attack.mitre.org/matrices/enterprise/cloud/officesuite/
- Matrice ATT&CK pour les services de fournisseurs d'identité type Microsoft Entra ID
  https://attack.mitre.org/matrices/enterprise/cloud/identityprovider/

5.2.5 Outillage

- Module PowerShell Azure AD incident Response
  https://github.com/AzureAD/Azure-AD-Incident-Response-PowerShell-Module
- Outil d'analyse 365Inspect
  https://github.com/soteria-security/365Inspect

5.3 Définitions

CC BY-NC-SA 4.0

5.3.1 Axes d'évaluation

- *Périmètre* : Le périmètre d'un incident désigne son étendue sur le système d'information et dans son administration.
- *Impact* : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- *Urgence* : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

5.3.2 Compromission d'un compte de messagerie

Une *compromission d'un compte de messagerie* désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

5.3.3 Compromission système

Une *compromission système* est l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, résultant en sa prise de contrôle.

Faute de pouvoir qualifier précisément la prise de contrôle, dans de nombreux cas, toute activité adverse sur le système pouvant avoir donné lieu à une escalade de privilège est considérée comme une compromission. Une compromission entraîne généralement une forme de communication entre la machine compromise et un attaquant y exécutant des actions.

5.3.4 Degrés de gravité

- *Anomalie courante* (gravité faible) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- *Incident mineur* (gravité modérée) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- *Incident majeur* (gravité élevée) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- *Crise cyber* (gravité critique) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

CC BY-NC-SA 4.0

5.3.5 Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

5.3.6 Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.

Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

5.3.7 Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- *Évaluer la gravité/priorité de l'incident* en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

5.4 Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.

CC BY-NC-SA 4.0

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT externe en prestation de réponse à incident	https://www.cybermalveillance.gouv.fr/diagnostic/accueil https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations
CERT sectoriel	https://www.cert-aviation.fr https://www.m-cert.fr https://esante.gouv.fr/produits-services/cert-sante	Pour les organisations du secteur de l'aviation, maritime ou santé
CERT-FR	Consulter la section Contacter le CERT-FR	Pour les administrations et les opérateurs d'importance vitale et de services essentiels

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise
- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

5.5 Déclarations

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

Qui ?	Comment ?	Pourquoi ?
Assureurs		Notifier son assurance cyber permet de démarrer la prise en compte de la couverture et d'identifier des prestataires que l'assureur pourra recommander ou mandater.
ANSSI	https://www.cert.ssi.gouv.fr/contact/ https://cyber.gouv.fr/notifications-reglementaires	L'administration, les opérateurs d'importance vitale et de services essentiels, et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI.
Dépôt de plainte	https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles	Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission même si aucune exfiltration de données n'a été confirmée.
Autres autorités		Une organisation d'un domaine réglementé (finance, santé, etc.) est astreinte à des obligations de déclaration spécifiques. Dans le doute, consulter le service juridique.

5.6 Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être préparée en amont, contextualisée et traduite en une *procédure interne et actionnable*

CC BY-NC-SA 4.0

immédiatement à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.

Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.

5.7 Contacter le CERT-FR

Attention

Quand vous effectuez un signalement auprès du CERT-FR, un numéro de référence vous est attribué. Pensez à rappeler ce numéro quand vous nous recontactez, ou dans l'entête de vos messages afin de simplifier le suivi du cas.

5.7.1 Par Téléphone

Le CERT-FR est joignable 7J/7, 24H/24 :

- depuis la France métropolitaine au **3218** (service gratuit + prix d'un appel) ou 09 70 83 32 18
- depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18

5.7.2 Par Internet

- mèl : `cert-fr@ssi.gouv.fr`
- site : `https://cert.ssi.gouv.fr/contact/`

5.7.3 Clé PGP du CERT-FR

Pour vérifier l'intégrité des informations fournies ci-dessous, veuillez contacter le CERT-FR.

Identifiant de la clé : `0x1B45CF2A`

Empreinte de la clé : `7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A`

Télécharger la clé publique : `https://cert.ssi.gouv.fr/uploads/public_key_2024.asc`

CC BY-NC-SA 4.0

5.8 Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT FRANCE

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (https://www.intercert-france.fr/publications/fiches-reflexes/).

Le présent document est publié sous licence CC BY-NC-SA 4.0.

ANSSI/SDO
Version 1- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr