PADSI
poste de travail sécurisé
by design

Sept. 2026

https://github.com/DGAC/padsi

Disclaimers

Les opinions exprimées sont les miennes, pas celle de mon employeur

Cette présentation parle de poste de travail Linux

Une simple question

Qu’est-ce que ≃ 99% des attaques via les postes de travail ont en commun ?

À l’exception des wipers et des attaques entièrement automatisées par IA

Point commun

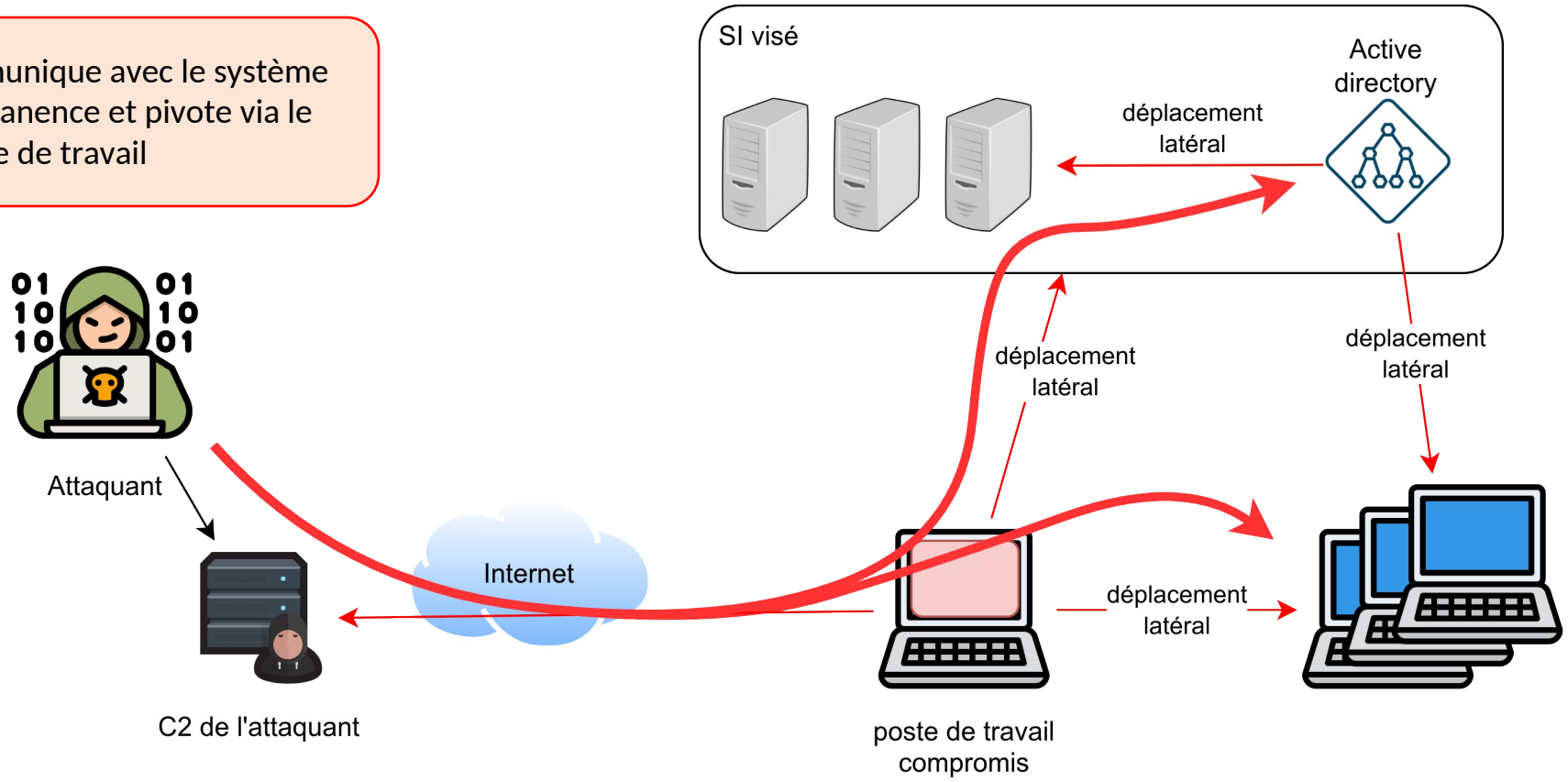
Qu’est-ce que ≃ 99% des attaques via les postes de travail ont en commun ?

Les attaquants communiquent avec le système attaqué, durant toute la durée de l’attaque, via leur infrastructure C2

À l’exception des wipers et des attaques entièrement automatisées par IA

Schéma actuel de compromission

L'attaquant communique avec le système attaqué en permanence et pivote via le poste de travail



Point de départ de la réflexion

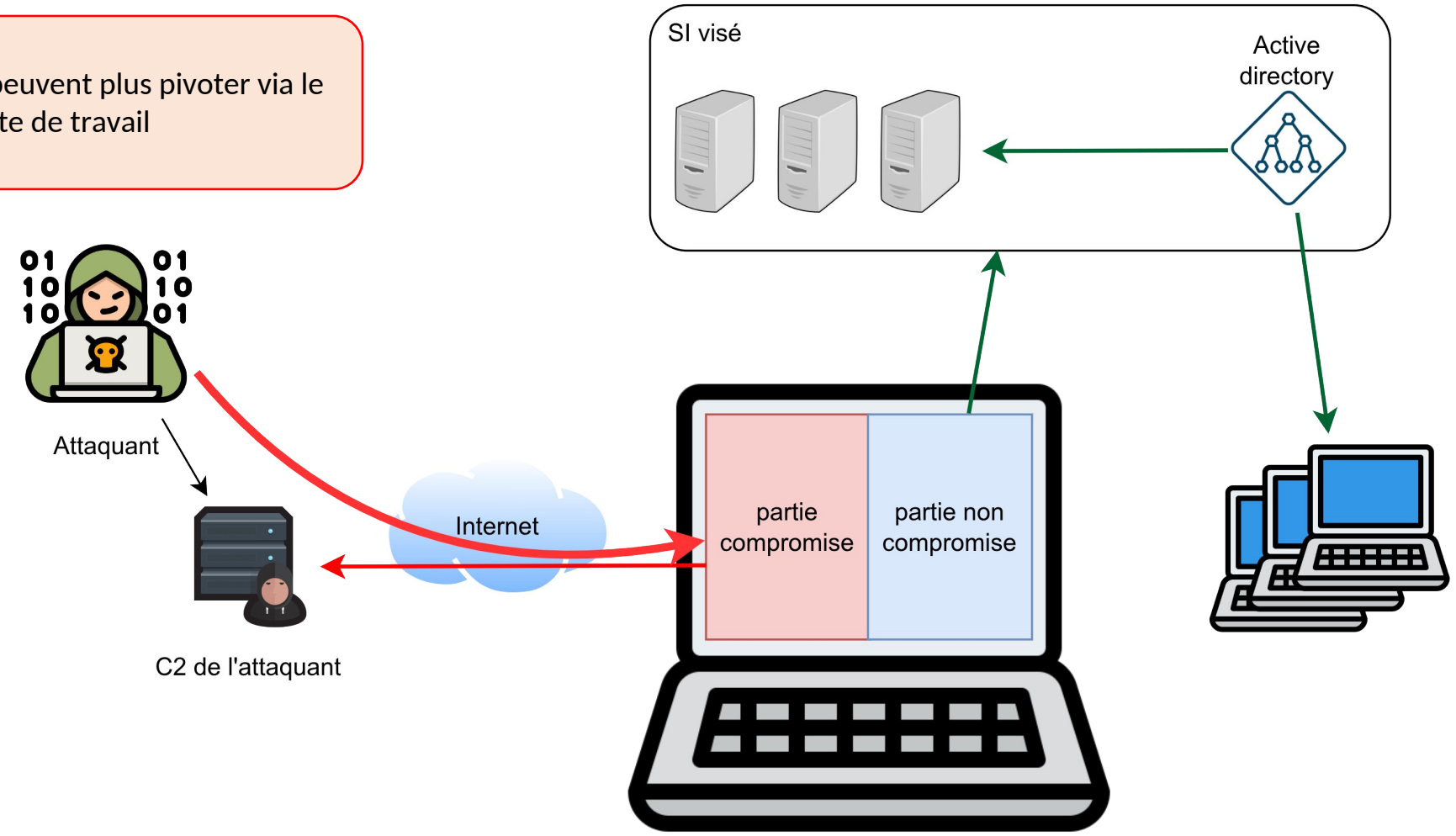
Les attaquants communiquent avec le système attaqué, durant toute la durée de l'attaque, via leur infrastructure C2

⇒ limiter les capacités de communications d'un attaquant avec son C2

C'est l'approche retenue par Qubes OS 

Limiter les capacités de communications

Le attaquant ne peuvent plus pivoter via le poste de travail



PADSI : objectifs et concepts

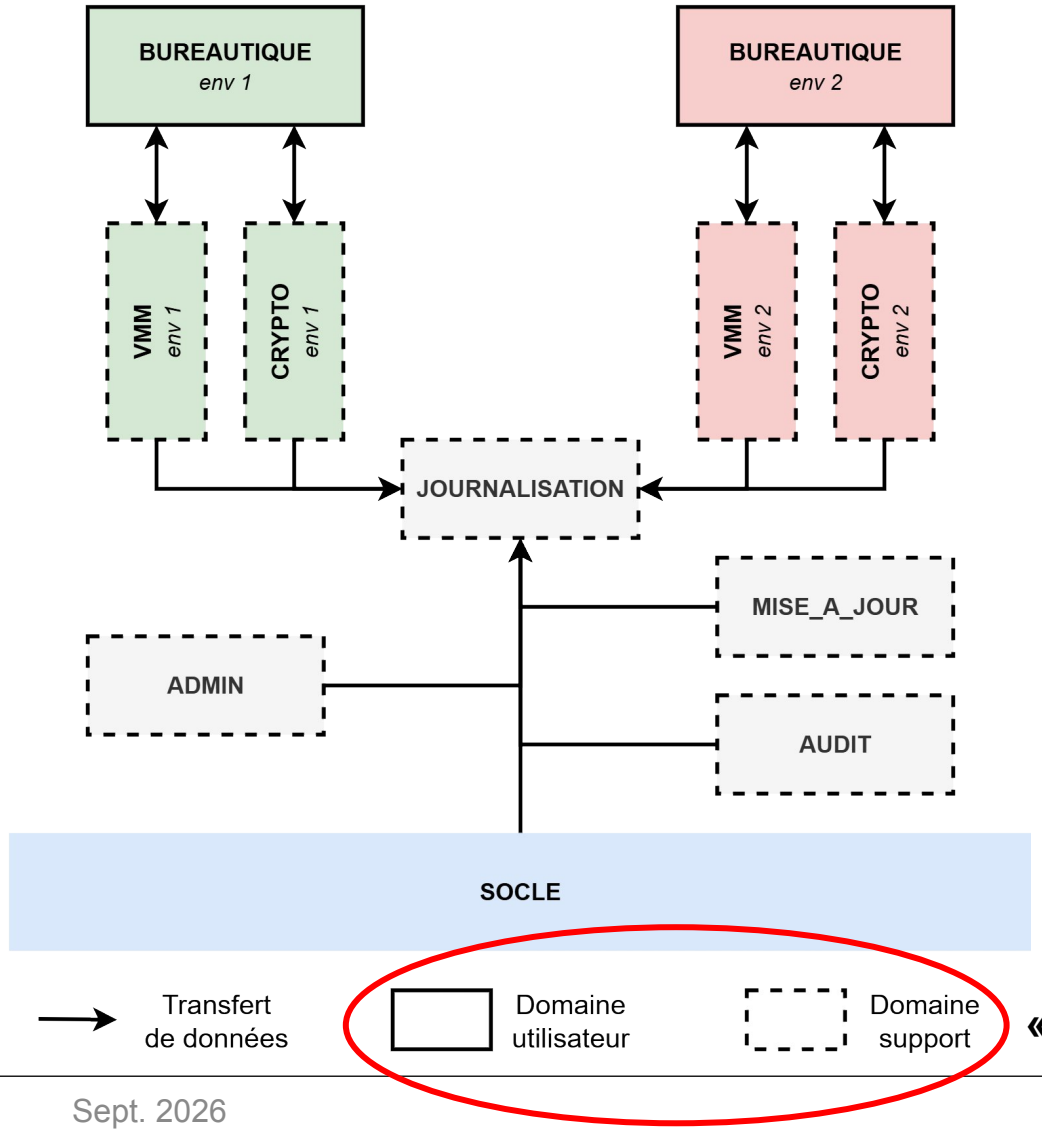
Objectifs :

- sécuriser les accès à certaines ressources
- prendre en compte les recommandation de l'ANSSI (postes multi-environnements)
- tolérer l'exécution de logiciel malveillant sur le poste avec un impact faible ou nul
- dégrader au minimum l'utilisabilité (pour les utilisateurs et les administrateurs des PC)
- ne pas créer une nouvelle distribution Linux

Concepts clé :

- **« zone »** : groupement d'activités métier ayant les mêmes besoins en terme d'accès à des fichiers ou à des ressources réseau
- sécurité en profondeur via de la micro segmentation : **isolation légère** via des « conteneurs » ou **isolation forte** via des machines virtuelles

Architecture recommandée par l'ANSSI



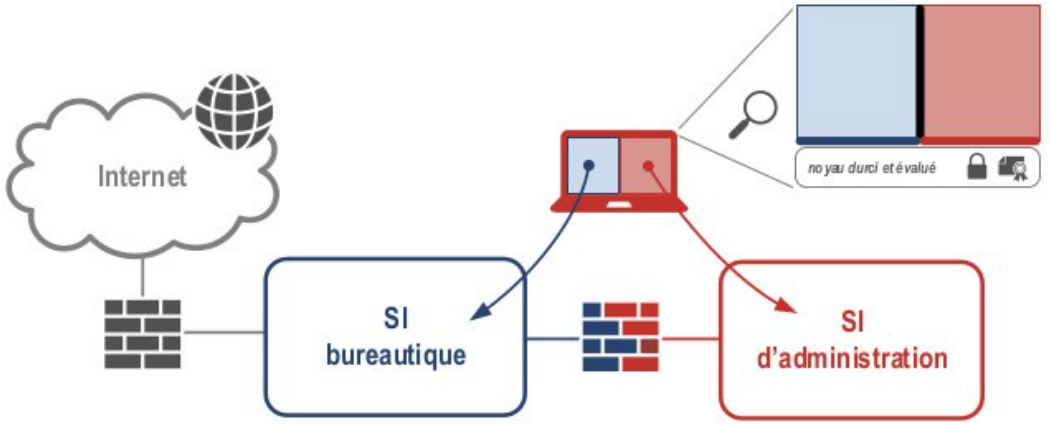
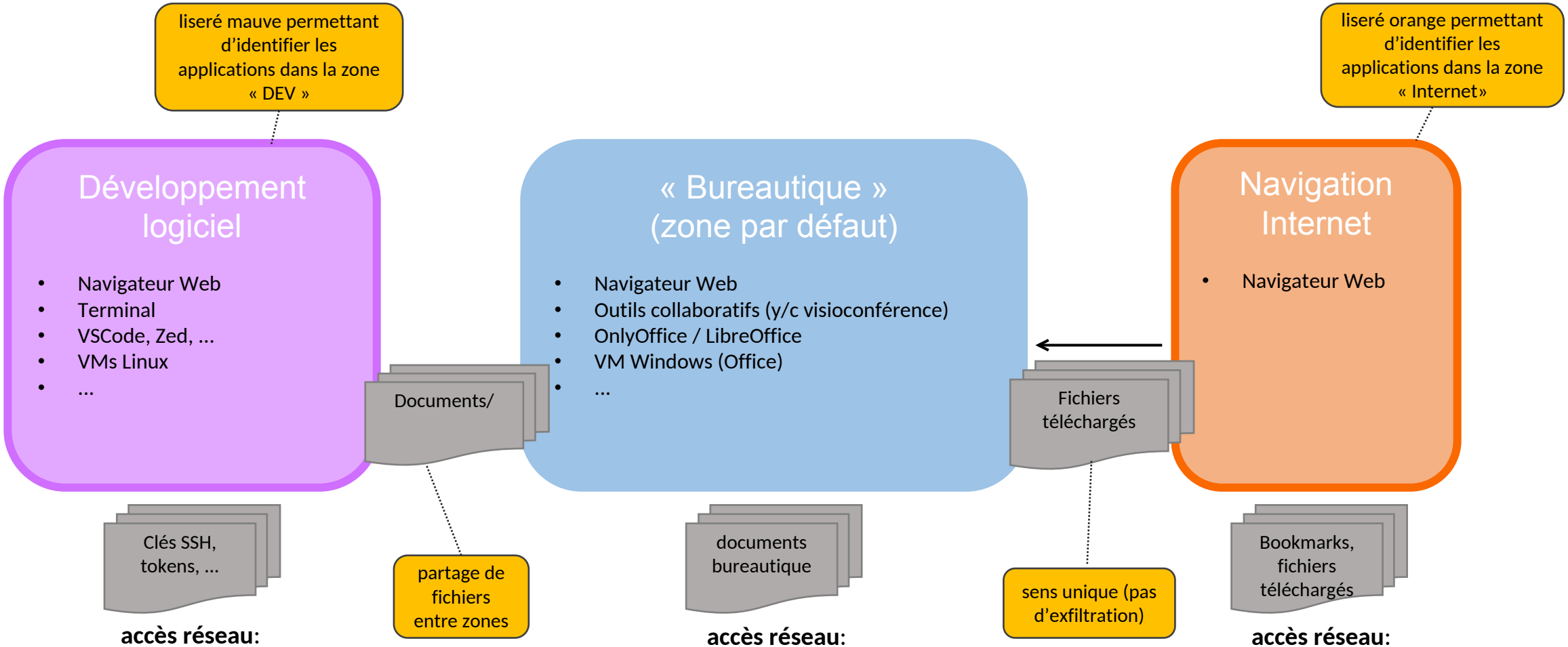


FIGURE 4.2 – Poste d'administration multi-niveaux

« domaine utilisateur » ≃ zone PADSI

Exemple de définition de zones



Efficacité illustrée

1. attaques : ransomware, info stealer, déplacement latéral…

Scenario 1.DEV

un attaquant exécute un programme malveillant dans la zone **DEV**

pas de communication avec le C2, y compris avec un système interne compromis

⇒ aucun impact

Scenario 1.bureautique

un attaquant exécute un programme malveillant dans la zone **bureautique**

pas de communication avec le C2, sauf potentiellement avec un système interne compromis

⇒ ~ aucun impact (supplémentaire)

Scenario 1.internet

un attaquant exécute un programme malveillant dans la zone **Internet**

communication avec le C2, mais pas avec le reste du SI

⇒ aucun impact

2. attaque : phishing

Scenario 2.DEV

l'utilisateur est redirigé vers une page de phishing via son navigateur dans la zone **DEV**

la page de phishing ne peut pas être chargée

⇒ aucun impact

Scenario 2.bureautique

l'utilisateur est redirigé vers une page de phishing via son navigateur dans la zone **bureautique**

la page de phishing ne peut *généralement* pas être chargée

⇒ ~ aucun impact

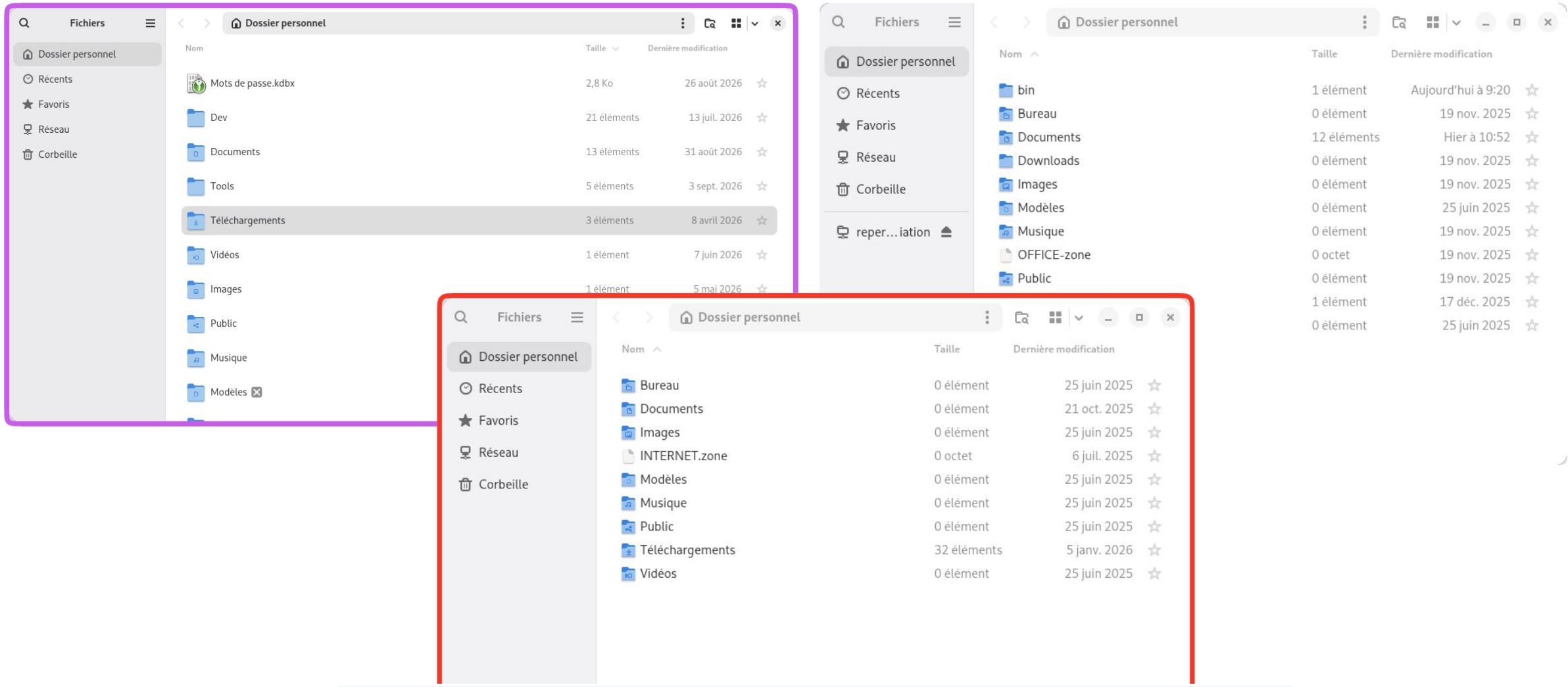
Scenario 2.internet

l'utilisateur est redirigé vers une page de phishing via son navigateur dans la zone **Internet**

la page de phishing est chargée mais l'utilisateur est informé qu'il ne doit *jamais*, *en aucun cas*, saisir de credentials dans le navigateur avec un liseré orange

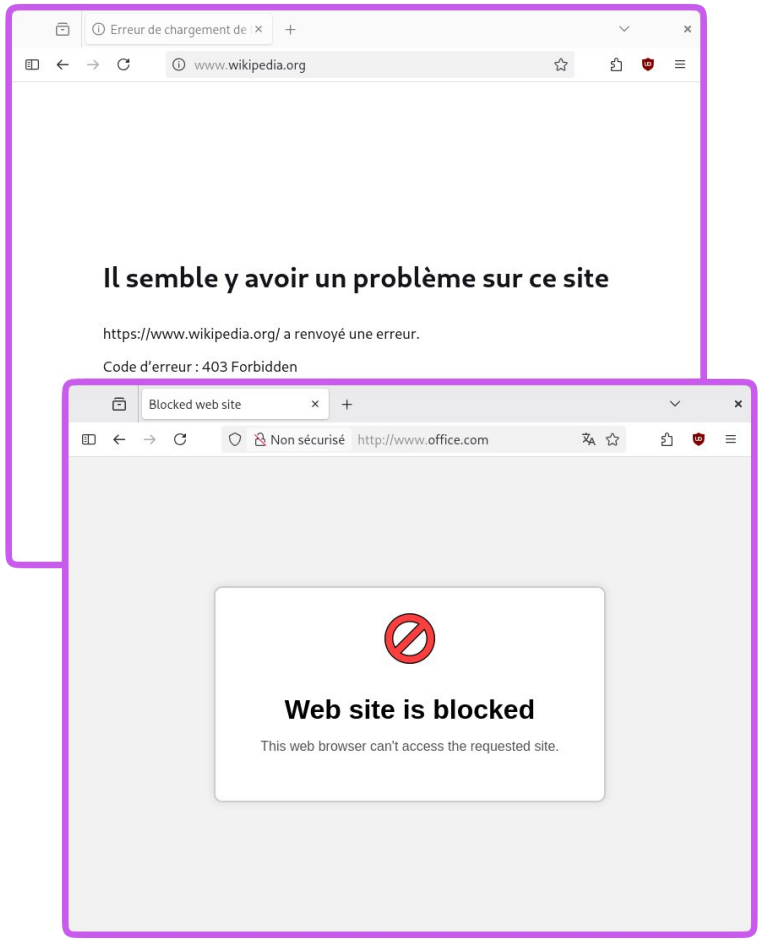
⇒ aucun impact

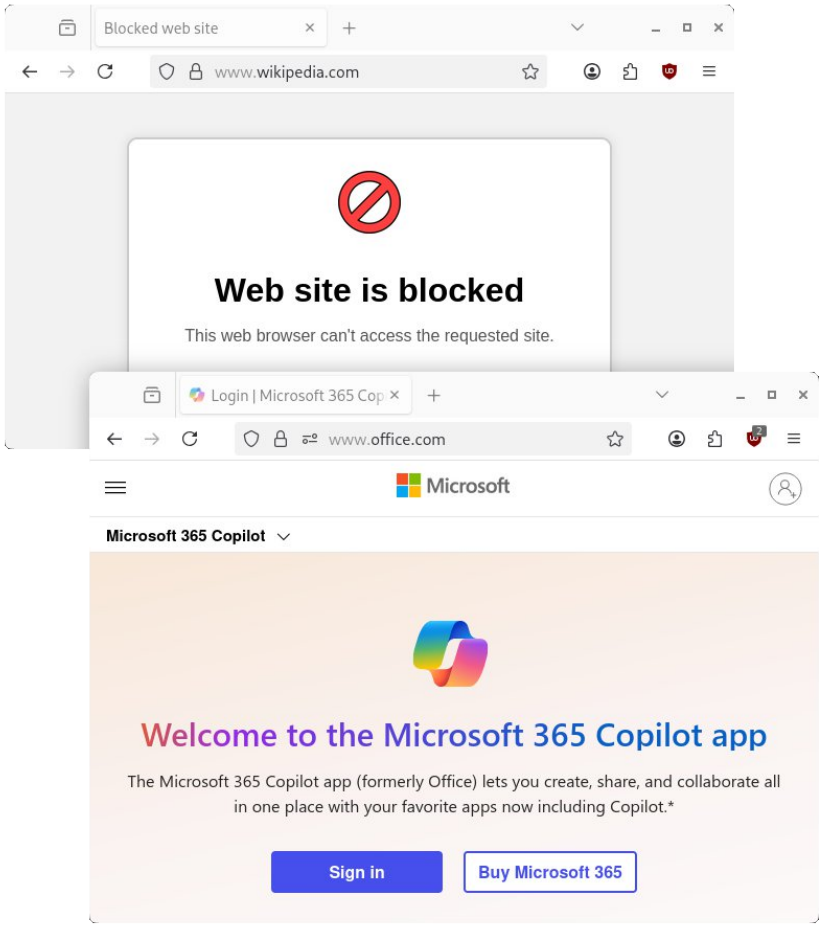
Travailler avec les zones

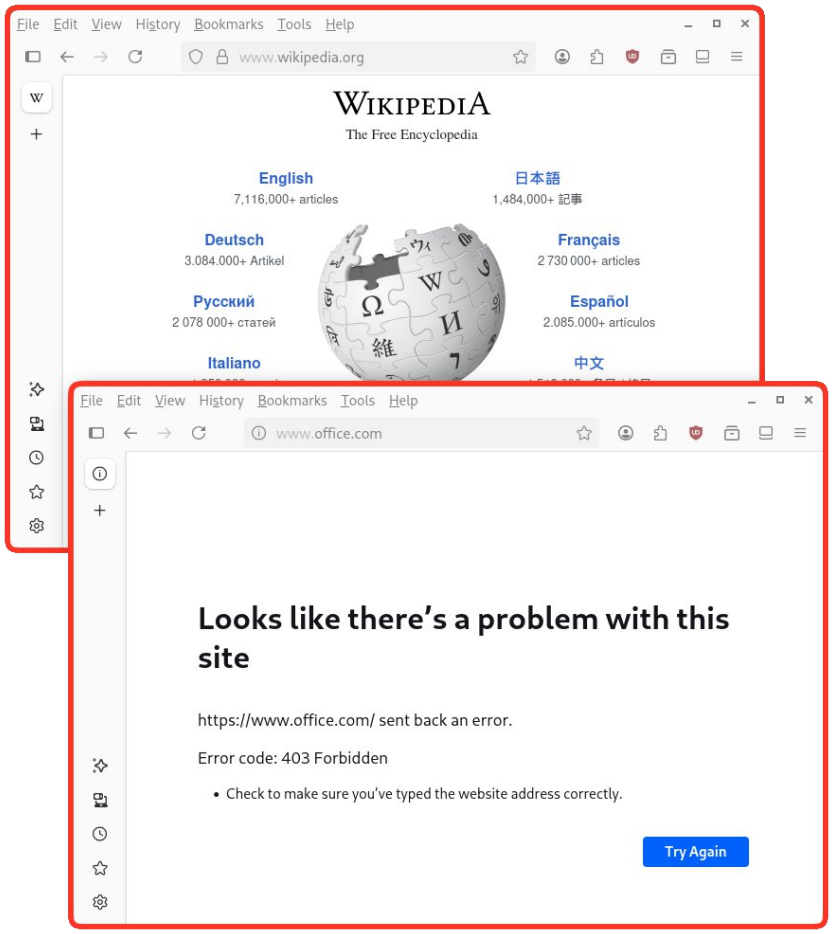


Gestionnaire de fichiers dans les 3 zones, contenus, paramétrages et partages réseau différents

Travailler avec les zones

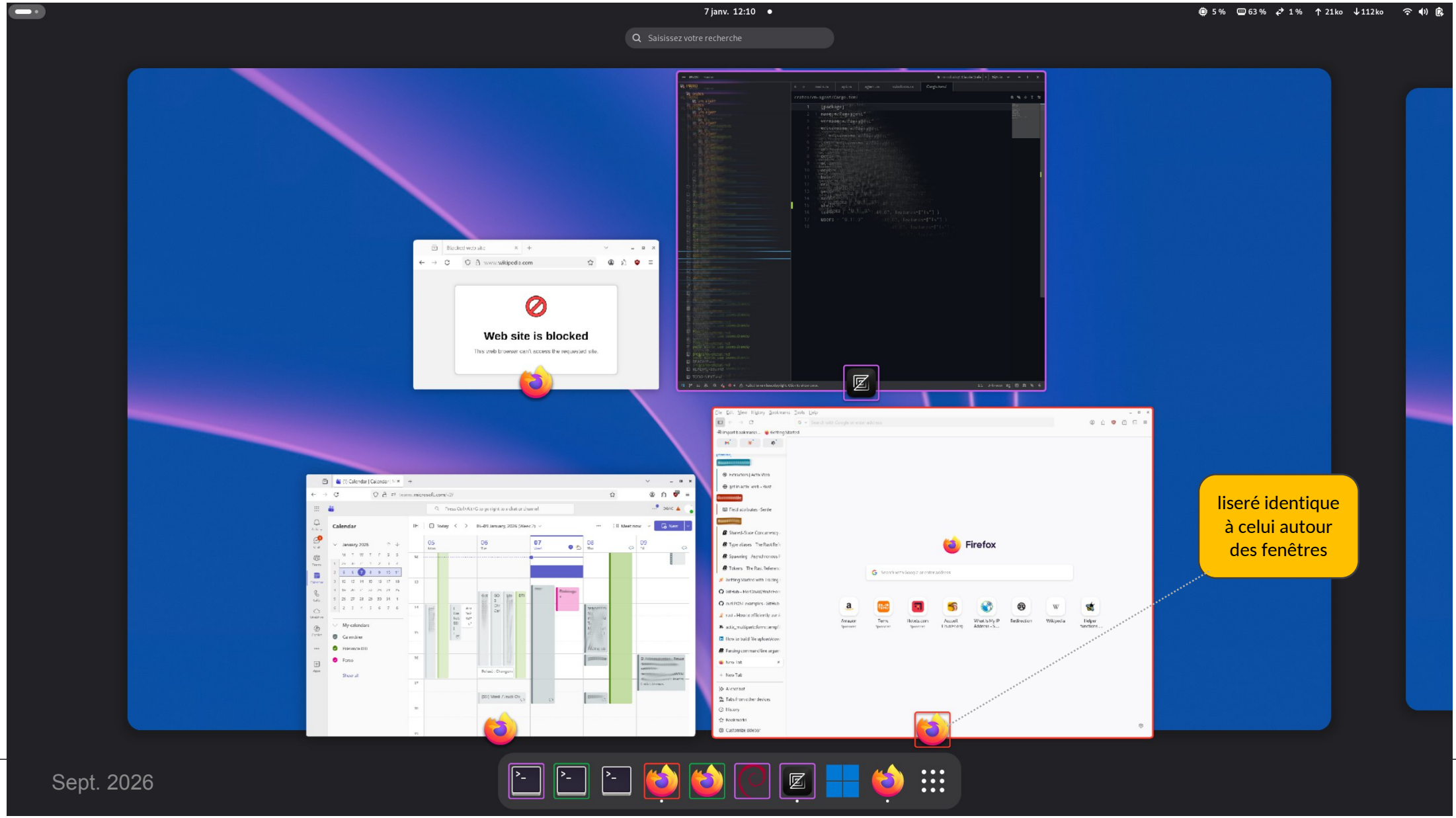






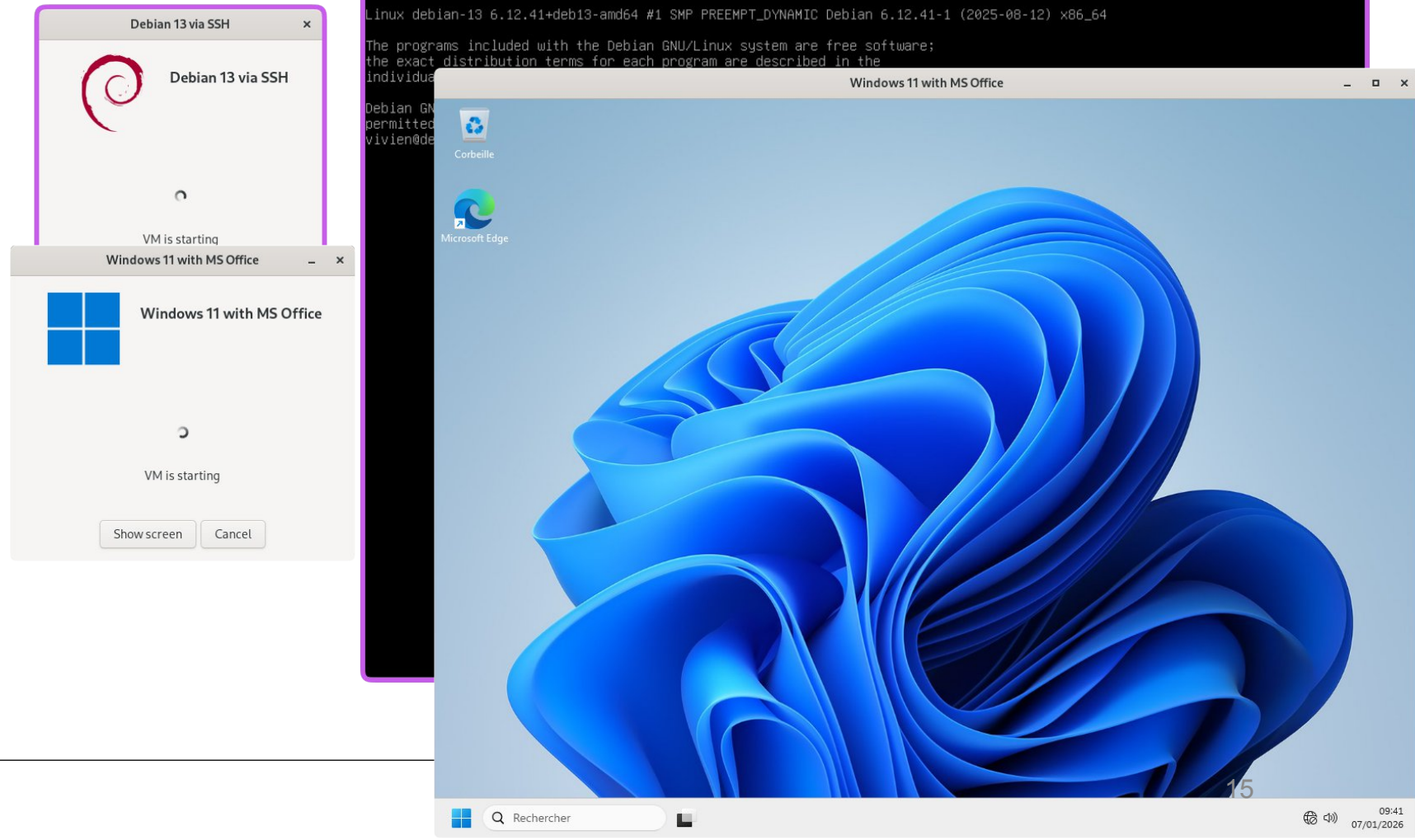
Chaque navigateur Web a des accès réseau différents

Vue d’ensemble et zones



Machines virtuelles

- double usage des VMs :
  - isolation forte entre zones
  - pour des besoins utilisateurs
- les VMs sont exécutées dans les zones, comme les programmes, et avec au moins les mêmes restrictions :
  - accès réseau
  - accès aux fichiers
- chaque VM est :
  - basée sur un « master »
  - spécialisée par utilisateur au 1er démarrage
  - exécutable en parallèle autant de fois que de besoin
  - exécutée avec ou sans IHM
- les VMs sont en réseau dans leur zone : <nom>.vm



Niveau de protection obtenu

Un système PADSI *correctement configuré* permet de se protéger très efficacement contre :

- le déplacement lateral,
- le vol de credential,
- les ransomware,
- le phishing,
- l'exfiltration de données,
- d'autres attaques reposant sur l'ingénierie sociale (ex. ClickFix)

Autres bénéfices:

- pas de dépendance à des services en SaaS (XDR, …) ⇒ protection contre leurs vulnérabilités intrinsèques,
- visibilité réseau extrêmement forte et fiable ⇒ meilleures capacités de détection
- VPN en mode « always ON », hors de maîtrise des utilisateurs, adresses IP statiques, facilité de gestion et capacités de sécurisation poussées,
- véritable « kill switch » VPN,
- pas besoin d'exposer les DNS internes lors de la navigateur Web Internet.

Note: le durcissement système, le MCS, la conformité sont à traiter par ailleurs

Roadmap

- ajouter d’une console de gestion (état des PC, application de politiques de sécurité),
- ajouter d’un système de sauvegarde adapté aux zones,
- ajouter d’une IHM de paramétrage et pour les utilisateurs (visibilité sur les flux réseau bloqués, gestion des VM, …),
- ajouter de la possibilité d’interception TLS locale pour permettre un filtrage Web plus précis (verbes HTTP, URL, certificats, …),
- permettre l’usage de réseaux accessible via un portail captif,
- permettre l’usage de puces TPM virtuelles dans les VM.

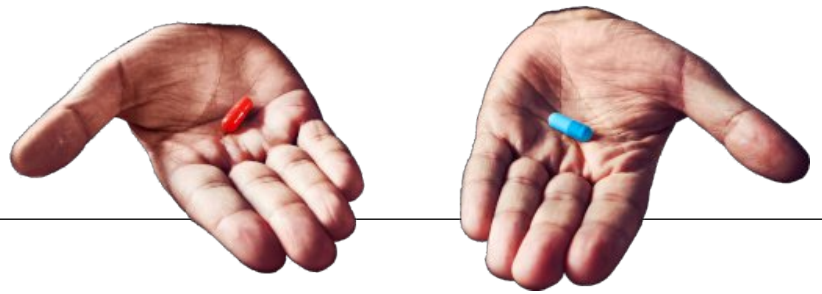
Opinion personnelle

PADSI est la démonstration qu'il est possible de construire un poste de travail sécurisé par conception, et à faible coût

Nous sommes à une période charnière, vous pouvez :

- vous atteler sérieusement à sécuriser les postes de travail, utiliser ou vous inspirer de PADSI
- briser la loi tacite qui impose Windows sur les postes de travail et (re)prendre le contrôle

- rester confortablement installé dans un schéma technique dont l'inefficacité est prouvée chaque jour
- en assumer les conséquences



Questions ?

https://github.com/DGAC/padsi

vivien.malerba@aviation-civile.gouv.fr