EXPERTISE TECHNIQUE EN SÉCURITÉ INFORMATIQUE

Sécurité des données d'un domaine Microsoft

GS Days – 28 Mars 2017

Sommaire

- Cogiceo
- Gestion des données
- Active Directory
- Méthodes de compromission
- Retours d'expérience
- Méthodologies de remédiation

Cogiceo

Cogiceo

- Fondé en 2012
- Audit technique en sécurité informatique
- Qualifié PASSI
- Organisme de formation
  - Certifiés Instructeurs SANS
- Orateurs et sponsors d'évènements
  - SSTIC, NSC, HxM, CRiP, OSSIR, FIC

Excellence

Indépendance

Expertise

Proximité

Expérience

Cogiceo

Nos offres

Audit

- Test d'intrusion
- Audit d'architecture
- Audit de code source
- Audit de configuration
- Audit organisationnel et physique

- Audit de domaine Microsoft
- Audit d'exposition Internet

Formation

- Formation développement web sécurisé
- Formation administration système sécurisée

- Sensibilisation de sécurité

Cogiceo

Nos clients

VEOLIA

orange

CRÉDIT AGRICOLE S.A.

SwissLife Banque Privée

GEODIS

SOCIETE GENERALE

SOCIETE GENERALE CALEDONIENNE DE BANQUE

AG2R LA MONDIALE

RETRAITE COMPLEMENTAIRE agirc et arrco

Groupe AGRICA

malakoff médéric

GROUPE BEAUMANOIR

CANAL+

Compagnie des Alpes

ORDRE NATIONAL DES MEDECINS Conseil National de l'Ordre

FG FONDS DE GARANTIE

DÉPARTEMENT DU GERS GASCOGNE

Strasbourg.eu eurométropole

TF1

Thai Union

GROUPE Semardel ENVIRONNEMENT SERVICE

Gestion des données

Gestion des données

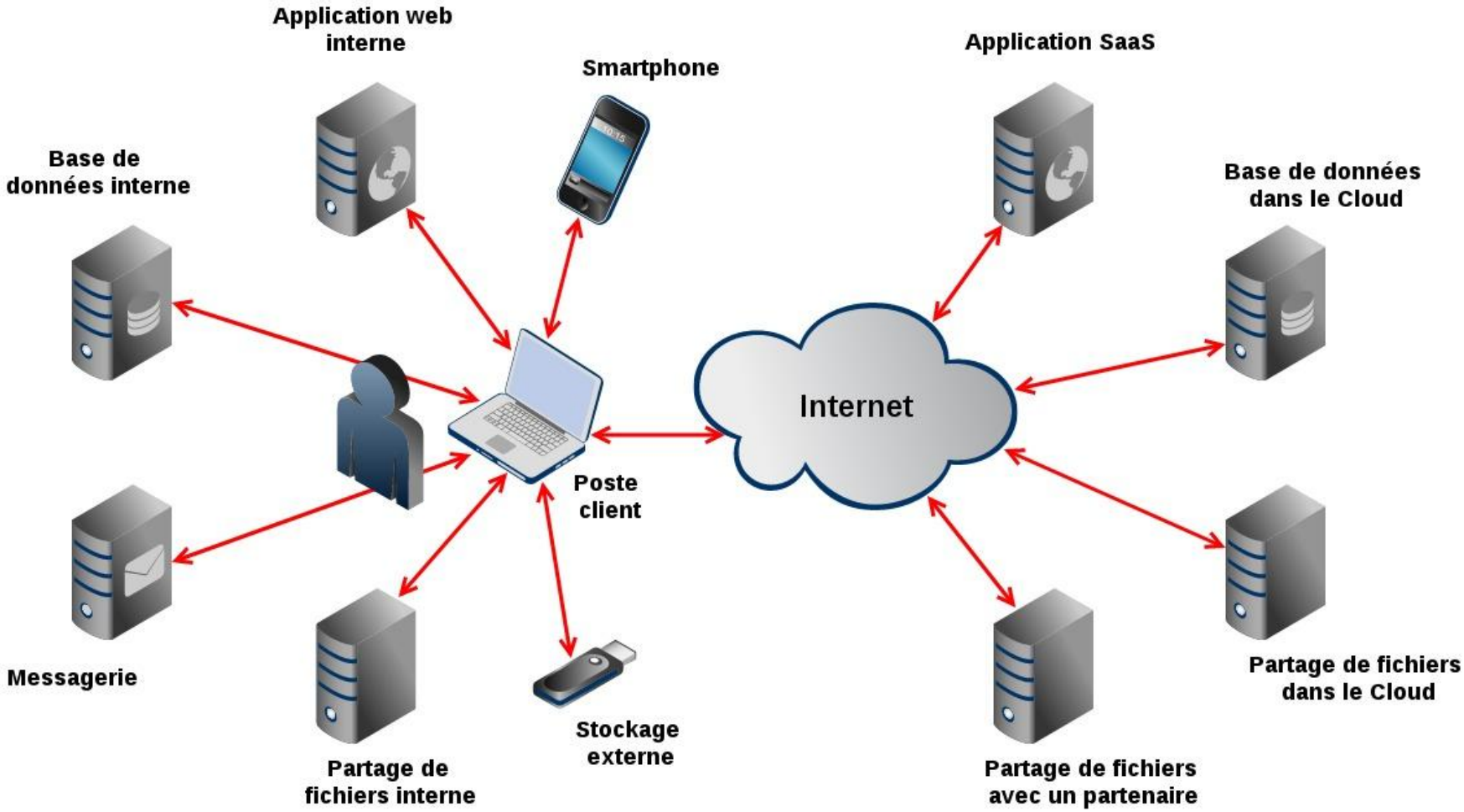
- Les données sont réparties dans le SI
  - Serveurs de stockage internes
  - Bases de données internes
  - Cloud
  - Postes clients
  - SI des partenaires
- Les données sont manipulées par de nombreux objets
  - Applications
  - Serveurs
  - Postes clients
  - Smartphones
- Les données ne sont pas chiffrées
  - Stockage
  - Flux réseau

Gestion des données

- Les accès à ces données sont centralisés
  - Active Directory
  - SSO
  - LDAP

- Depuis le poste client
  - Accès aux applications métiers
  - Accès à la messagerie
  - Accès au partage de fichiers
  - Accès au Cloud

Gestion des données



Active Directory

Active Directory

Domaine Microsoft

- Services d'annuaire
  - Identification
  - **Authentification**
- Objets
  - Utilisateurs, groupes, OU
  - **Machines**
  - Configurations, stratégies
- **Relations** d'approbation
  - Forêt

Constats

- **Criticité** de l'AD
  - Admins de domaine ont un accès absolu aux données des applications supportées par les serveurs
- Analyse manuelle **fastidieuse**
  - Multiplicité des données
  - Hétérogénéité des données
- **Pluralité** des attaques
  - Compromission direct
  - Compromission par rebond
  - Compromission par rejeu

Active Directory

Architecture sécurisée

- Inventorier et qualifier les données
  - systèmes, utilisateurs, applications
- Stratégie du « least-privilege »
- Ne jamais administrer un système avec un système de confiance inférieure
  - Utiliser l'authentification forte pour les tâches d'administration
- Sécuriser physiquement les équipements
- Renforcer la sécurité des comptes à hauts privilèges
  - Mode Administrateur Restreint, groupe « Utilisateurs Protégés »
- Renforcer la sécurité des contrôleurs de domaine
  - Read-Only Domain Controller (RODC), liste blanche des applications
- Mettre en place un système de contrôle automatique
  - Advanced Audit Policy

Active Directory

Architecture sécurisée

- Mettre à jour les applications
- Mettre à jour les systèmes d'exploitation
- Déployer et mettre à jour les antivirus et antimalware sur l'ensemble de systèmes et auditer les tentatives de suppression ou désactivation de ces logiciels
- Renforcer la sécurité des comptes utilisateurs qui ont accès à des données sensibles
- Empêcher les comptes sensibles à se connecter sur des systèmes non autorisés
- Isoler ou décommissionner les systèmes obsolètes
- Simplifier la sécurité pour les utilisateurs finaux

Active Directory

Constats

- La gestion des privilèges n'est pas assez fine dans les organisations
- Les paramétrages par défaut privilégient la compatibilité au détriment de la sécurité
- L'exploitation d'un domaine ne nécessite que peu de compétences; sa sécurité, en revanche, en demande nettement plus
- L'hyperconnectivité des SI d'un groupe implique souvent la compromission de l'ensemble à partir de la prise de contrôle d'un seul domaine

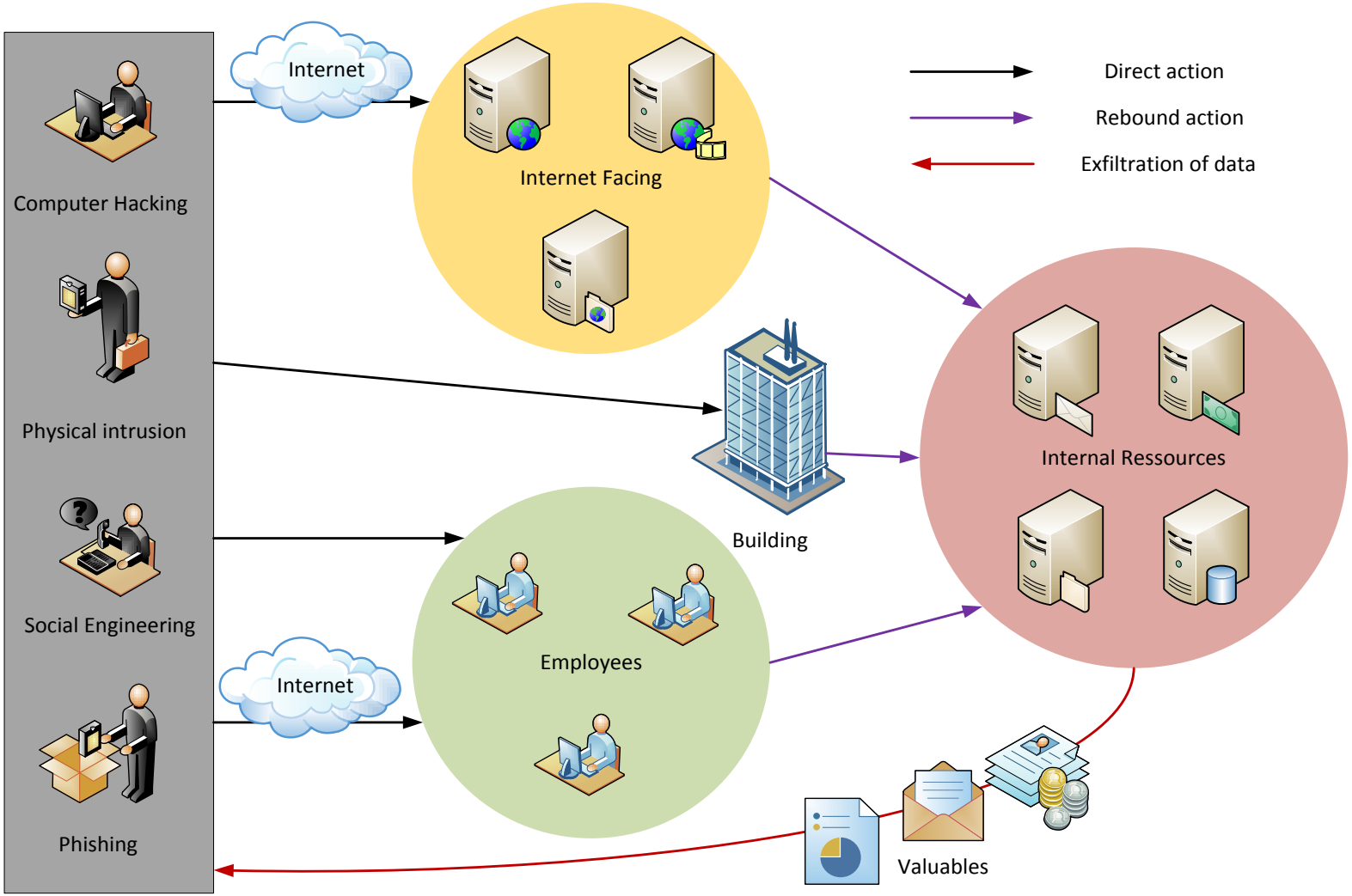
Méthodes de compromission

Méthodes de compromission

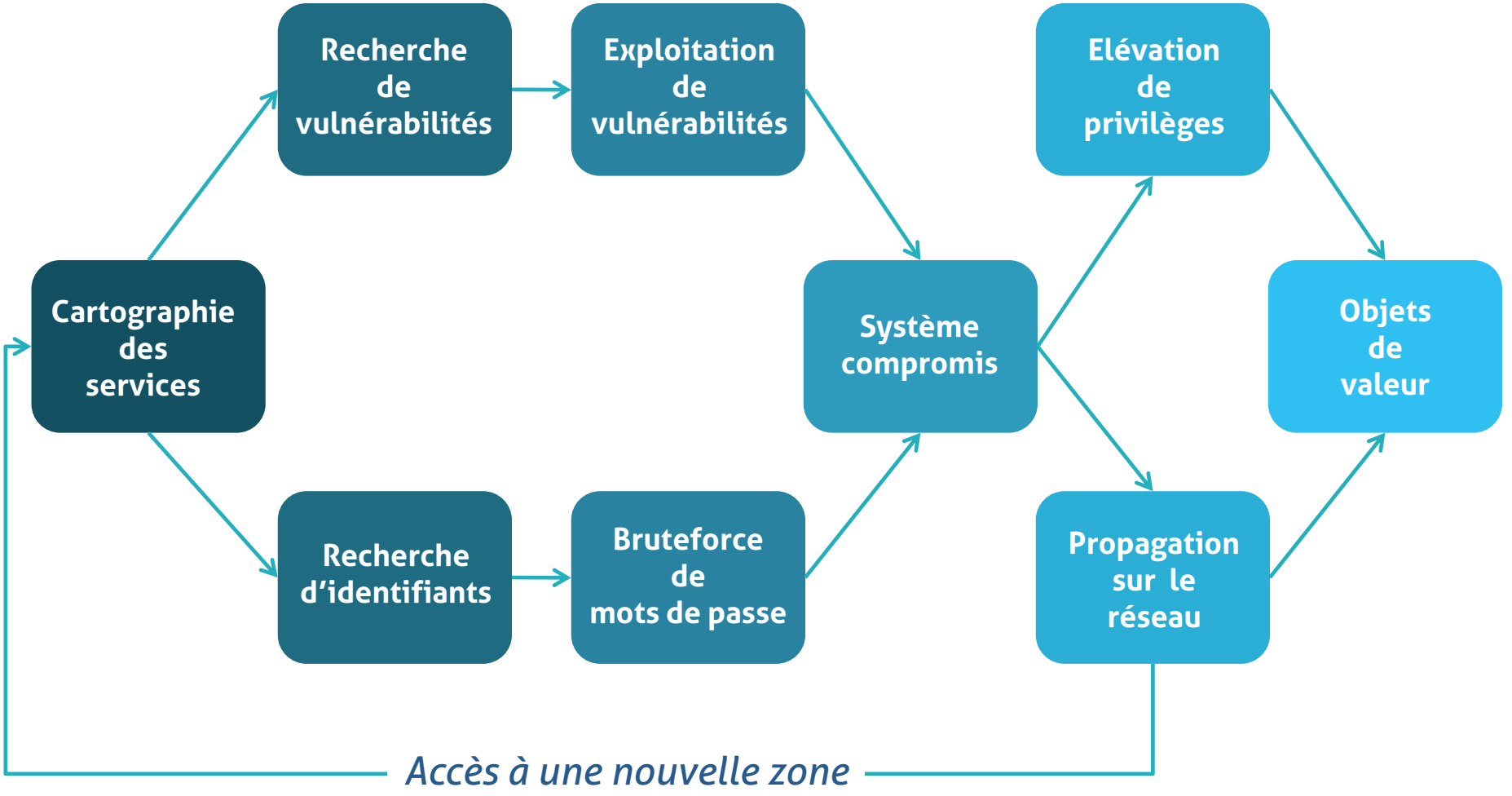
- Démarrage de la compromission d'un domaine
  - Attaques de services du SI disponibles sur Internet
  - Intrusion physique dans un bâtiment
  - Piégeage d'employés

- Tests d'intrusion internes
  - Compromission du domaine dans **100%** des cas
  - Moins de **6h** en moyenne
  - Peu de détections par les IDS
  - Peu de détections par les SOC

Méthodes de compromission

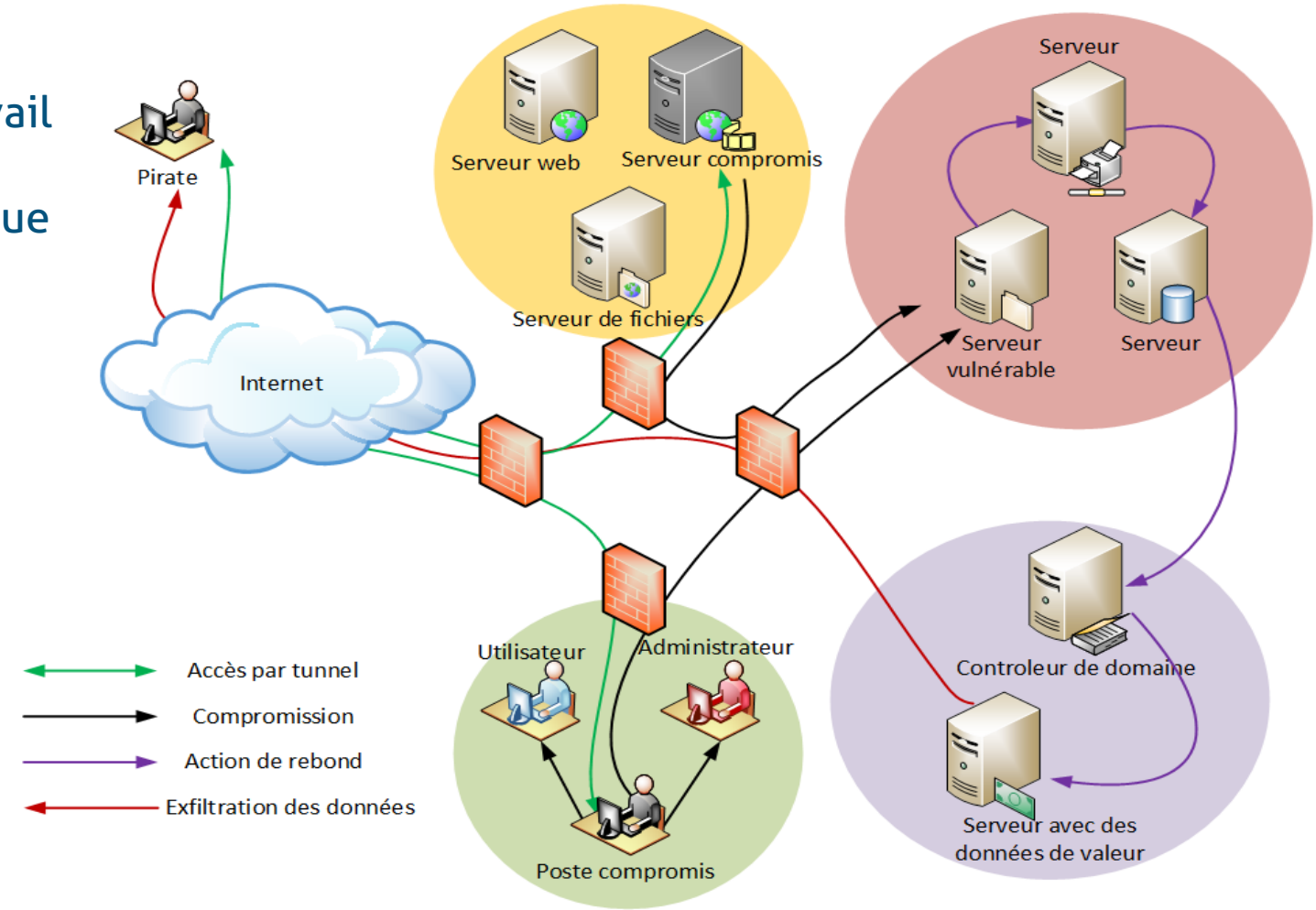


Méthodes de compromission



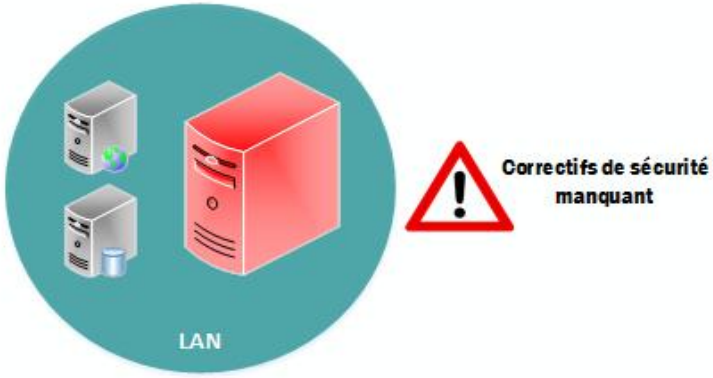
Méthodes de compromission

1. Serveur exposé sur Internet
2. Poste de travail
3. Accès physique



Méthodes de compromission

Gestion des mises à jour

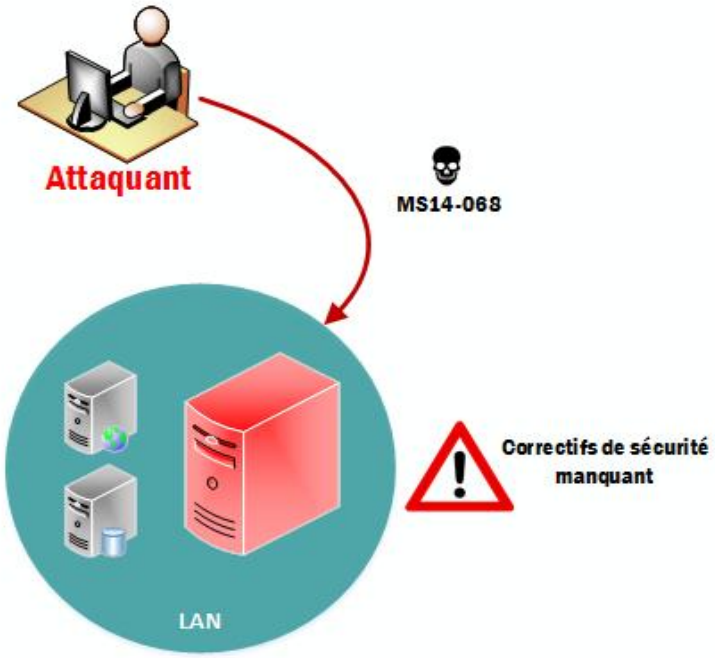


Vulnérabilité

- Plusieurs correctifs de sécurité critiques n'ont pas été appliqués sur un contrôleur de domaine

Méthodes de compromission

Gestion des mises à jour



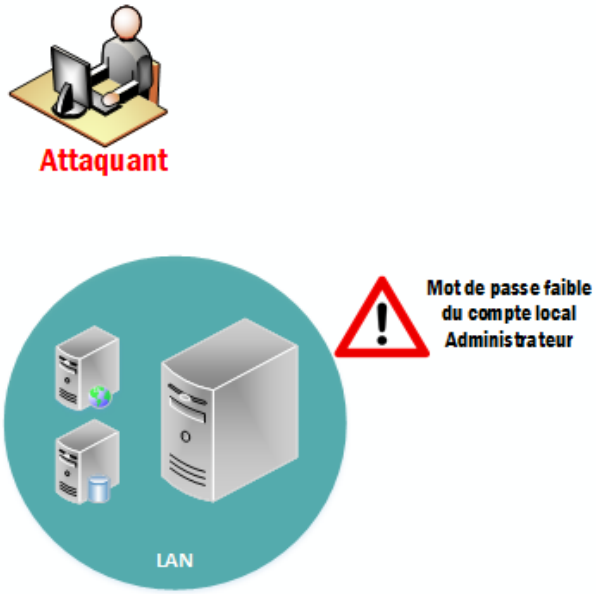
Déroulement de l'attaque

- La vulnérabilité MS14-068, affectant Kerberos, permet d'élever ses privilèges sur le domaine

- A partir d'un compte utilisateur standard, l'attaquant obtient alors les droits absolus sur le domaine

Méthodes de compromission

Gestion des mots de passe



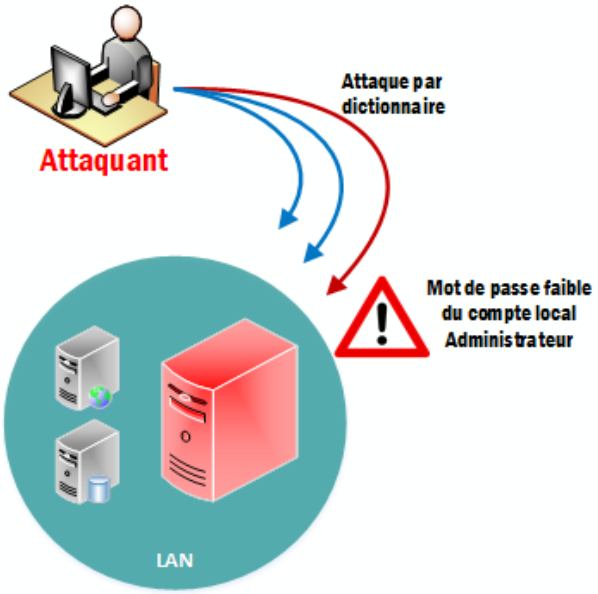
Vulnérabilités

- Plusieurs comptes locaux d'administration possèdent un mot de passe faible

- Un administrateur de domaine utilise le même mot de passe qu'un compte local d'utilisateur

Méthodes de compromission

Gestion des mots de passe



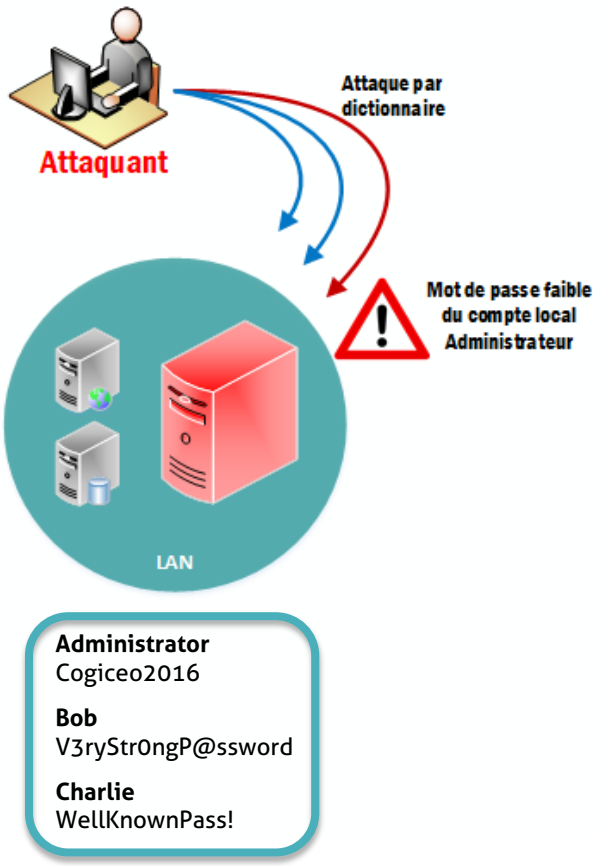
Déroulement de l'attaque

1. L'attaquant tente des identifiants prédictibles sur les serveurs du domaine

2. Il obtient alors les droits d'administration sur un serveur

Méthodes de compromission

Gestion des mots de passe

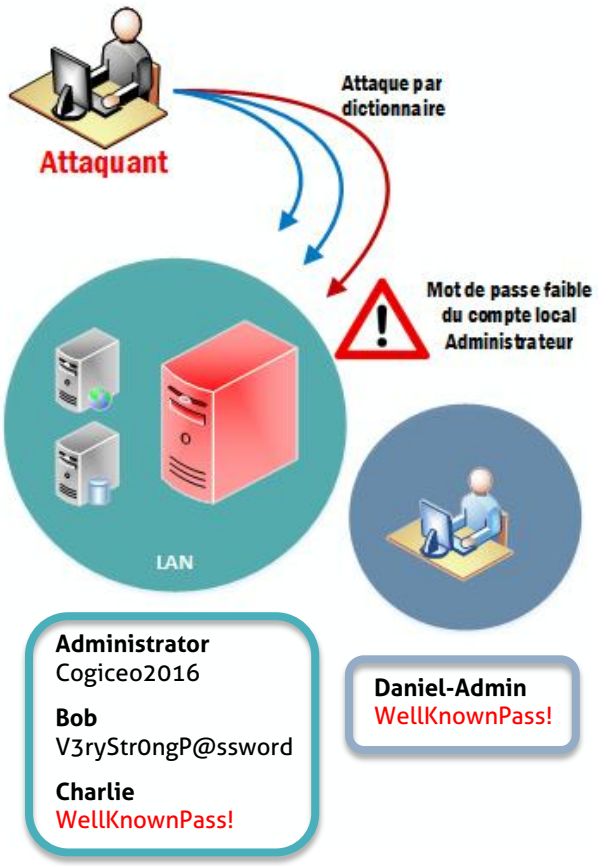


Déroulement de l'attaque

1. L'attaquant tente des identifiants prédictibles sur les serveurs du domaine
2. Il obtient alors les droits d'administration sur un serveur
3. L'attaquant extrait l'ensemble des comptes locaux du serveur

Méthodes de compromission

Gestion des mots de passe

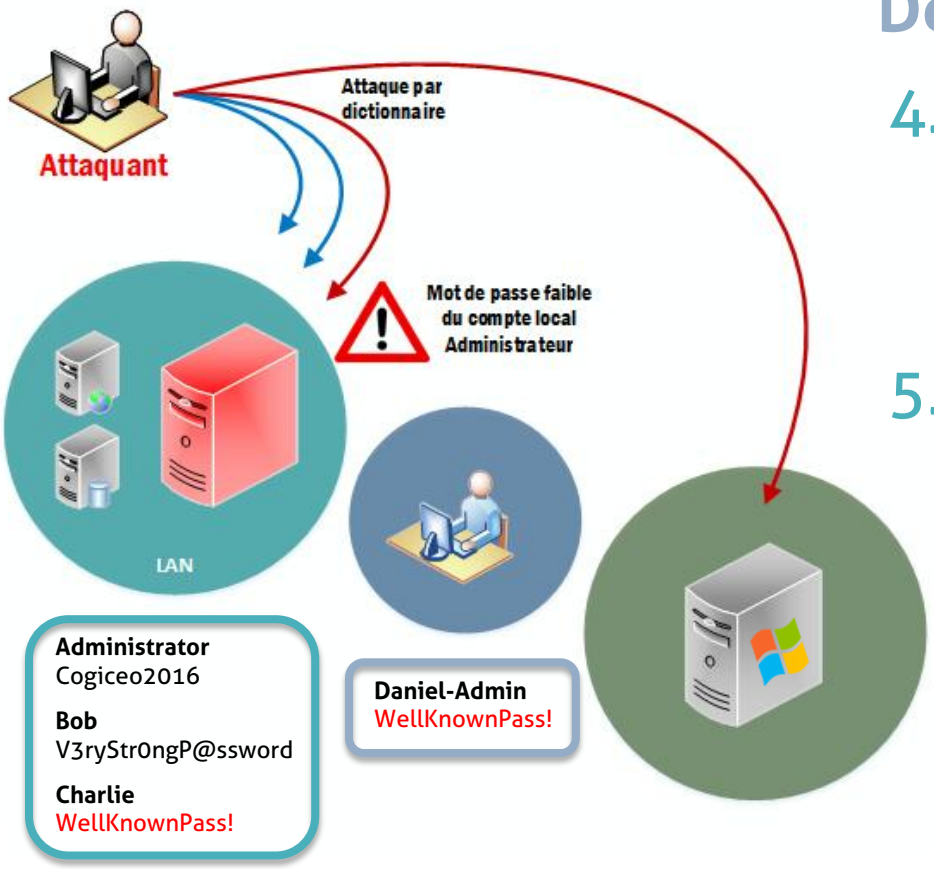


Déroulement de l'attaque

4. L'attaquant rejoue les mots de passe sur les comptes d'administration du domaine

Méthodes de compromission

Gestion des mots de passe



Déroulement de l'attaque

4. L'attaquant rejoue les mots de passe sur les comptes d'administration du domaine

5. Il obtient les droits absolus sur le domaine

Méthodes de compromission

Gestion des configurations de sécurité

Vulnérabilités

- Protocoles de nommage secondaires activés
- Droits permissifs sur des exécutables
- Services utilisant des comptes utilisateurs de domaine

Méthodes de compromission

Gestion des configurations de sécurité

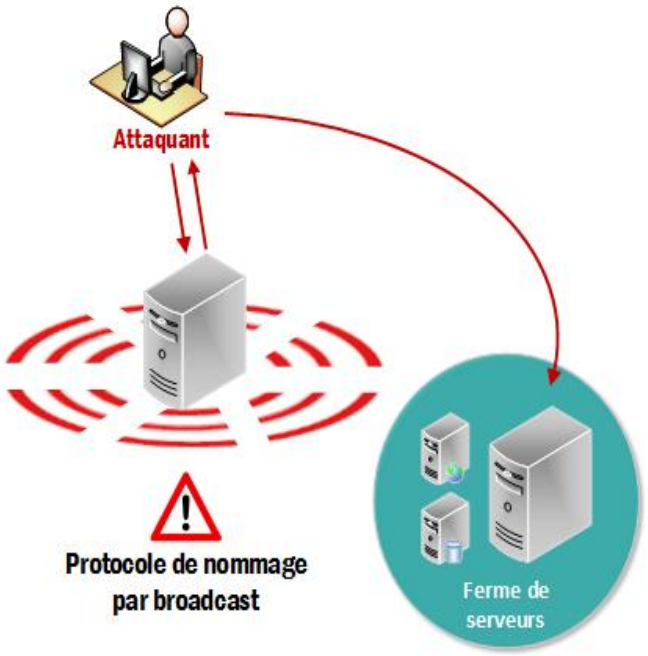
Déroulement de l'attaque

1. L'attaquant intercepte plusieurs authentifications NTLM

2. Après cassage, il obtient des identifiants de domaine

Méthodes de compromission

Gestion des configurations de sécurité

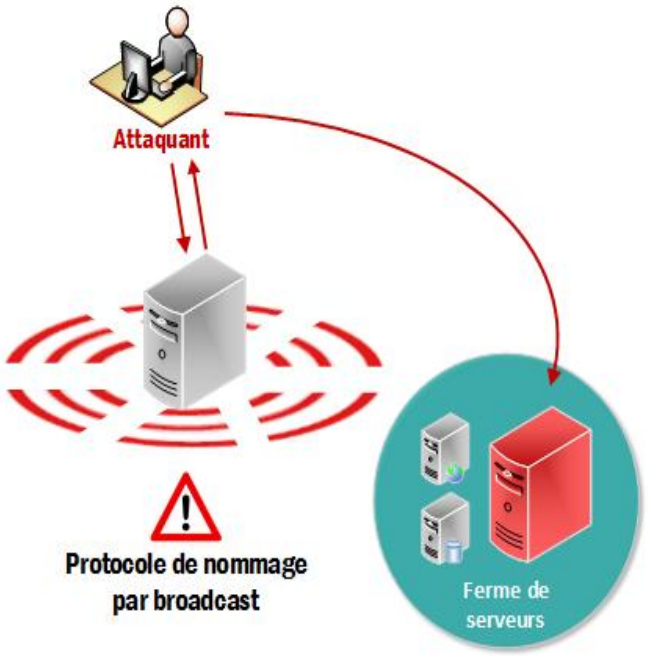


Déroulement de l'attaque

1. L'attaquant intercepte plusieurs authentifications NTLM
2. Après cassage, il obtient des identifiants de domaine
3. L'attaquant s'authentifie sur un serveur intégré dans le domaine

Méthodes de compromission

Gestion des configurations de sécurité

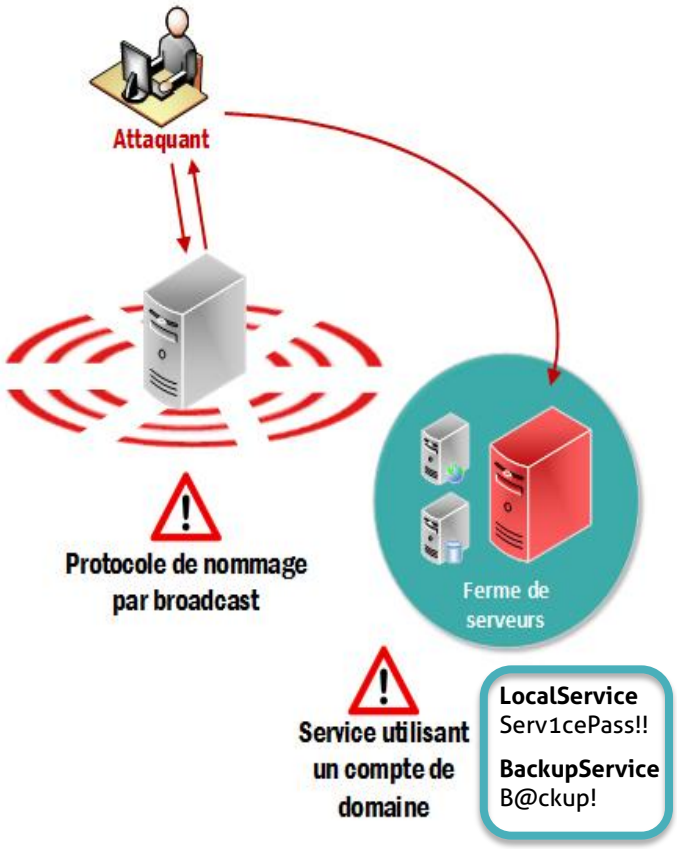


Déroulement de l'attaque

4. L'attaquant élève ses privilèges, exploitant des droits permissifs sur des exécutables

Méthodes de compromission

Gestion des configurations de sécurité



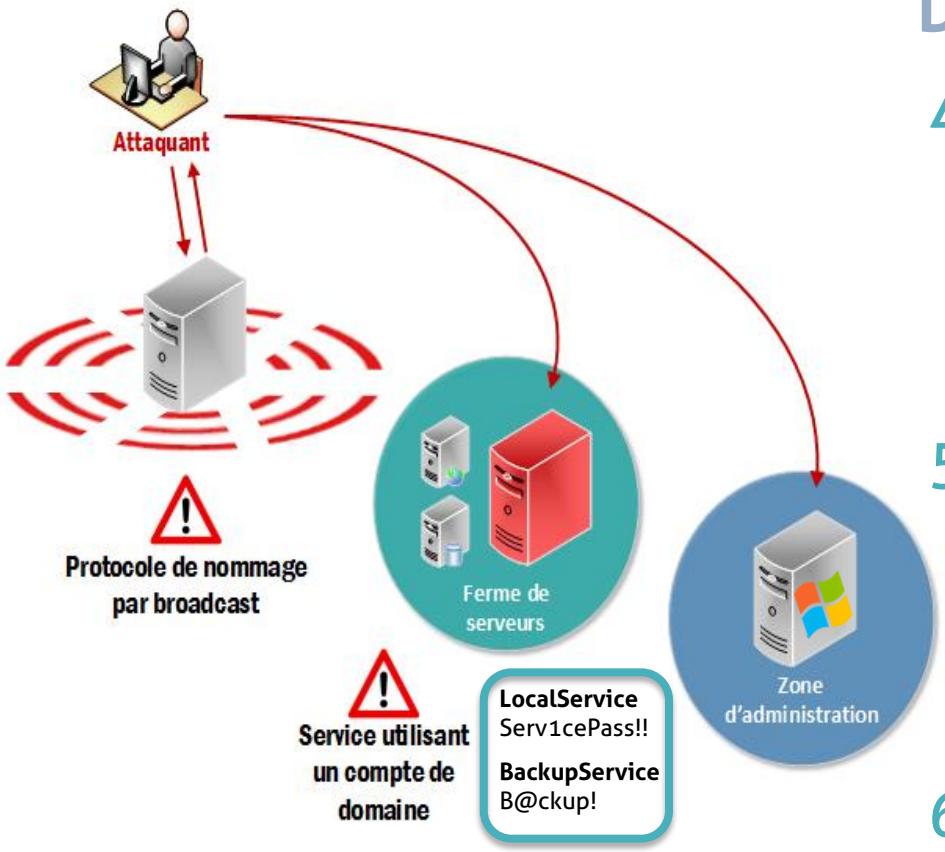
Déroulement de l'attaque

4. L'attaquant élève ses privilèges, exploitant des droits permissifs sur des exécutables

5. Il extrait les mots de passe des services utilisant des comptes administrateurs de domaine

Méthodes de compromission

Gestion des configurations de sécurité



Déroulement de l'attaque

4. L'attaquant élève ses privilèges, exploitant des droits permissifs sur des exécutables

5. Il extrait les mots de passe des services utilisant des comptes administrateurs de domaine

6. L'attaquant obtient les droits absolus sur le domaine

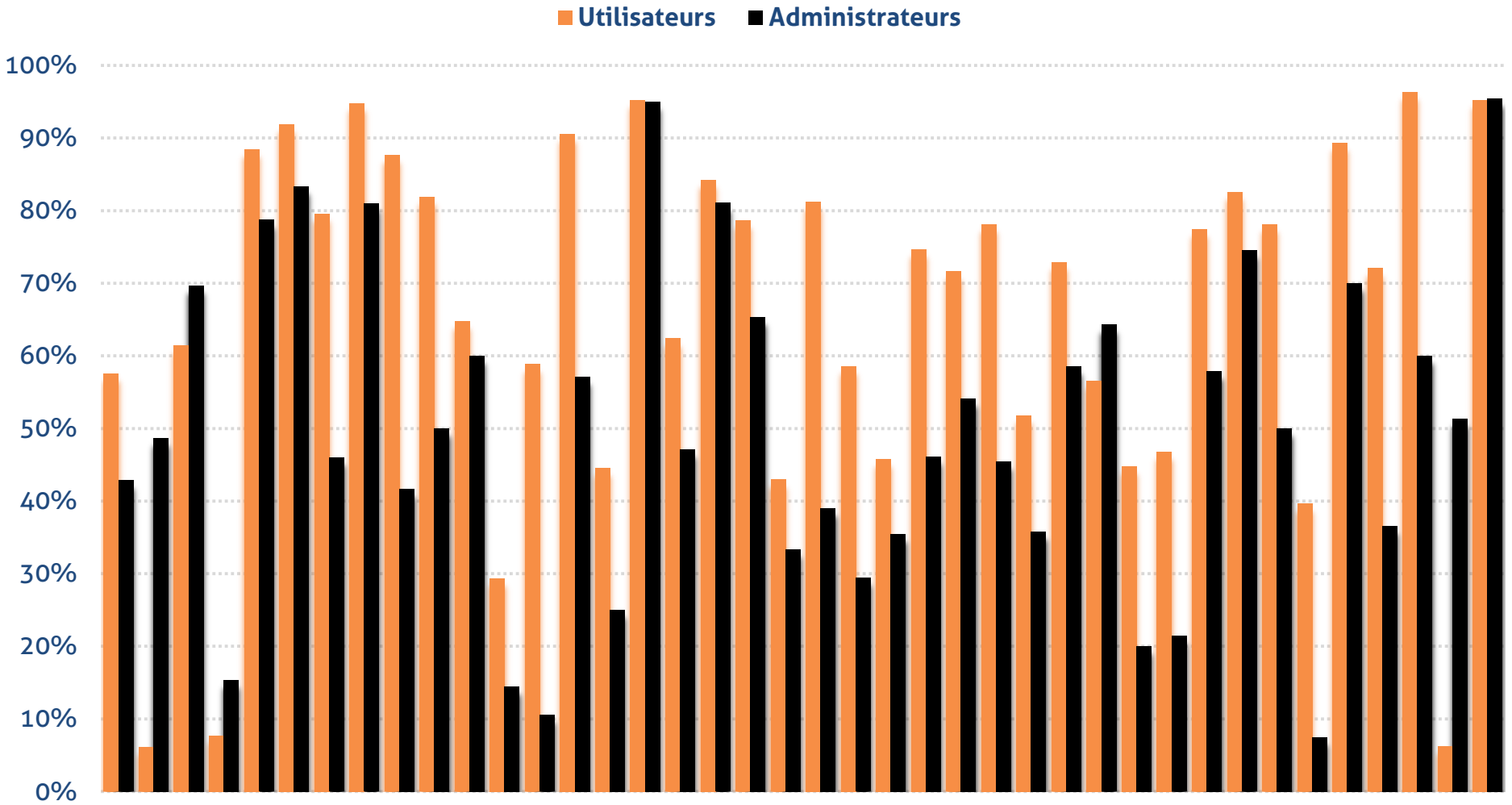
Retours d'expérience

Retours d'expérience

Echantillons

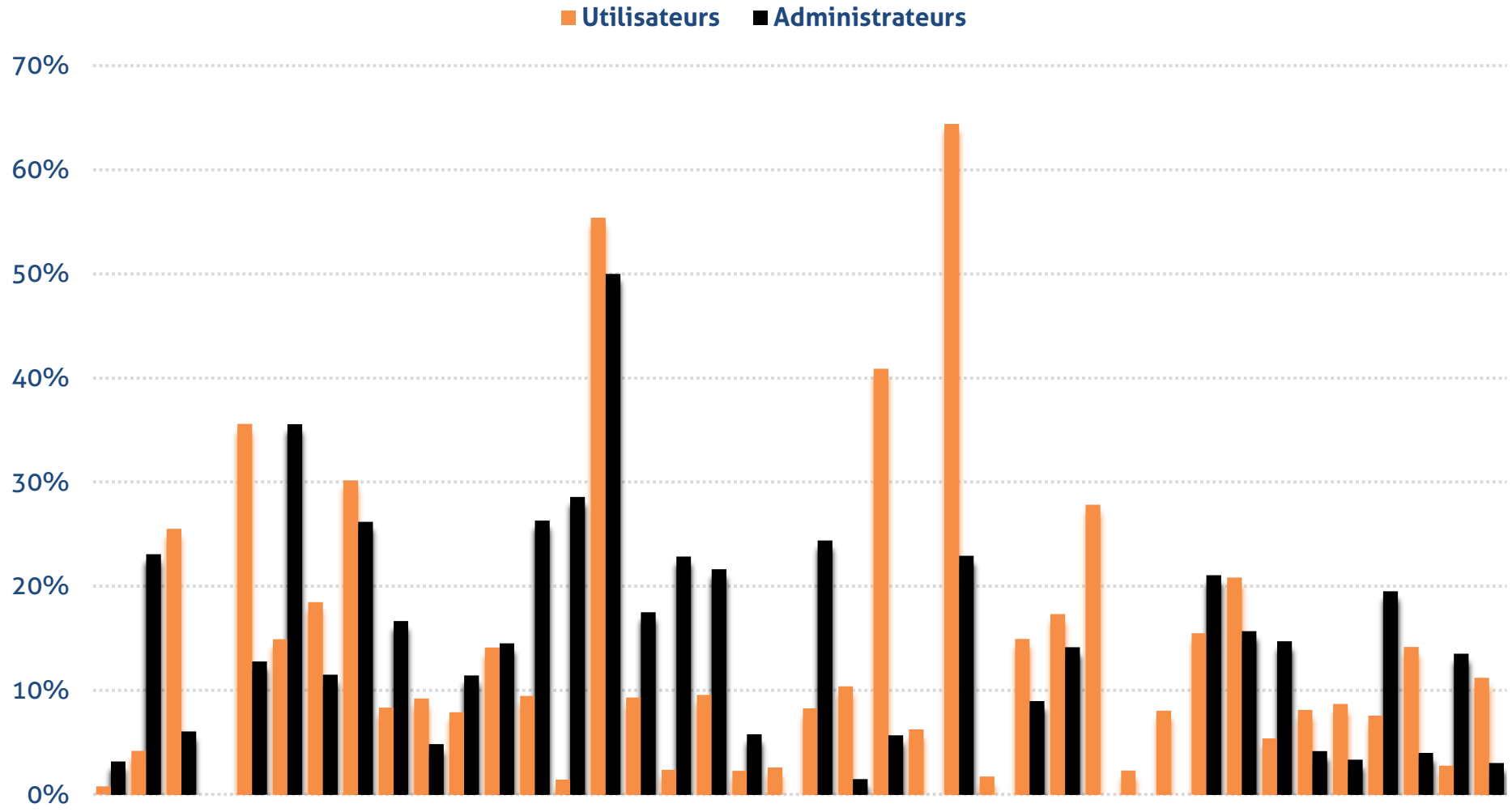
Retours d'expérience

Mots de passe



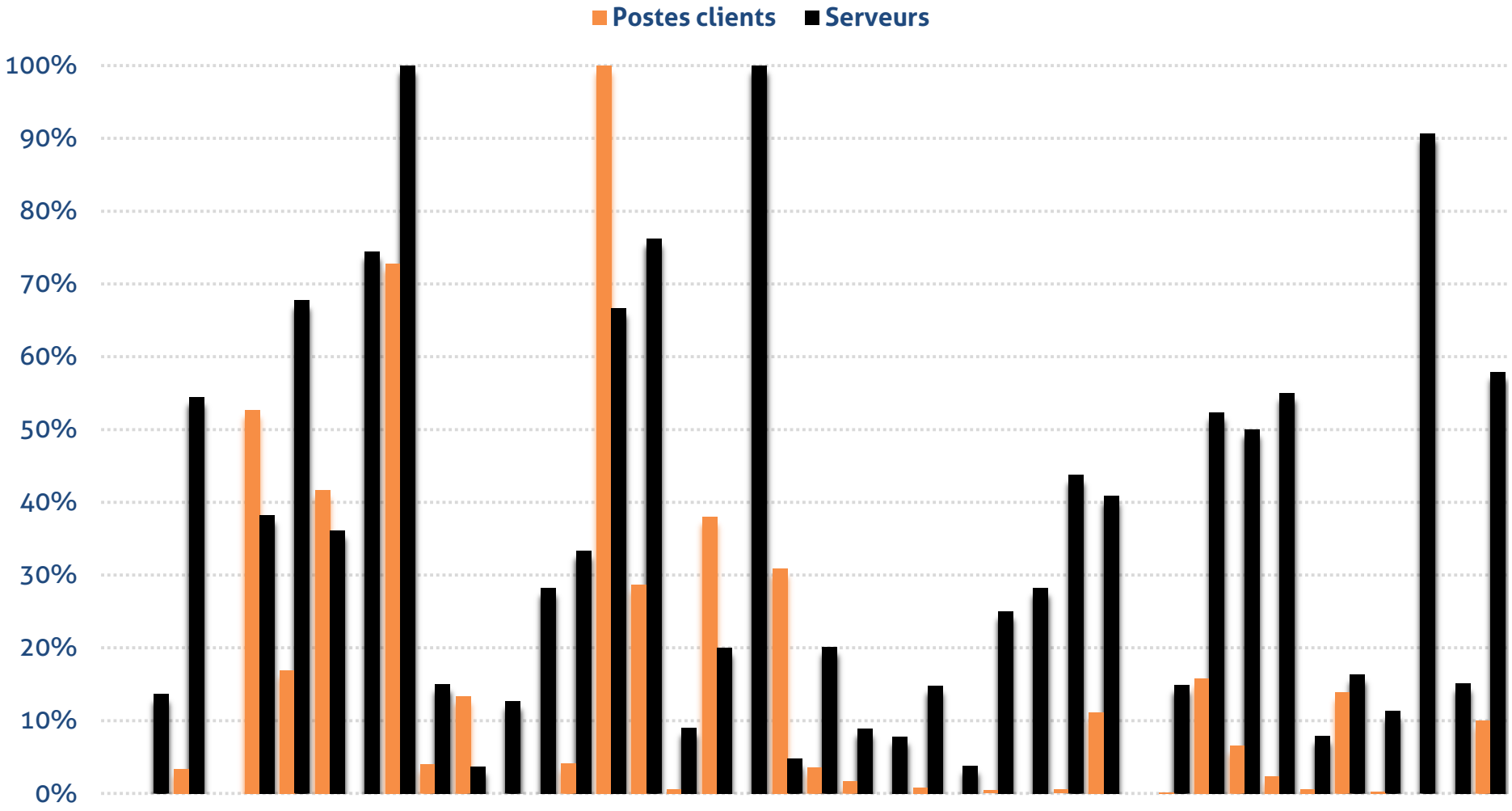
Retours d'expérience

Comptes oubliés, non connectés depuis plus de 13 mois



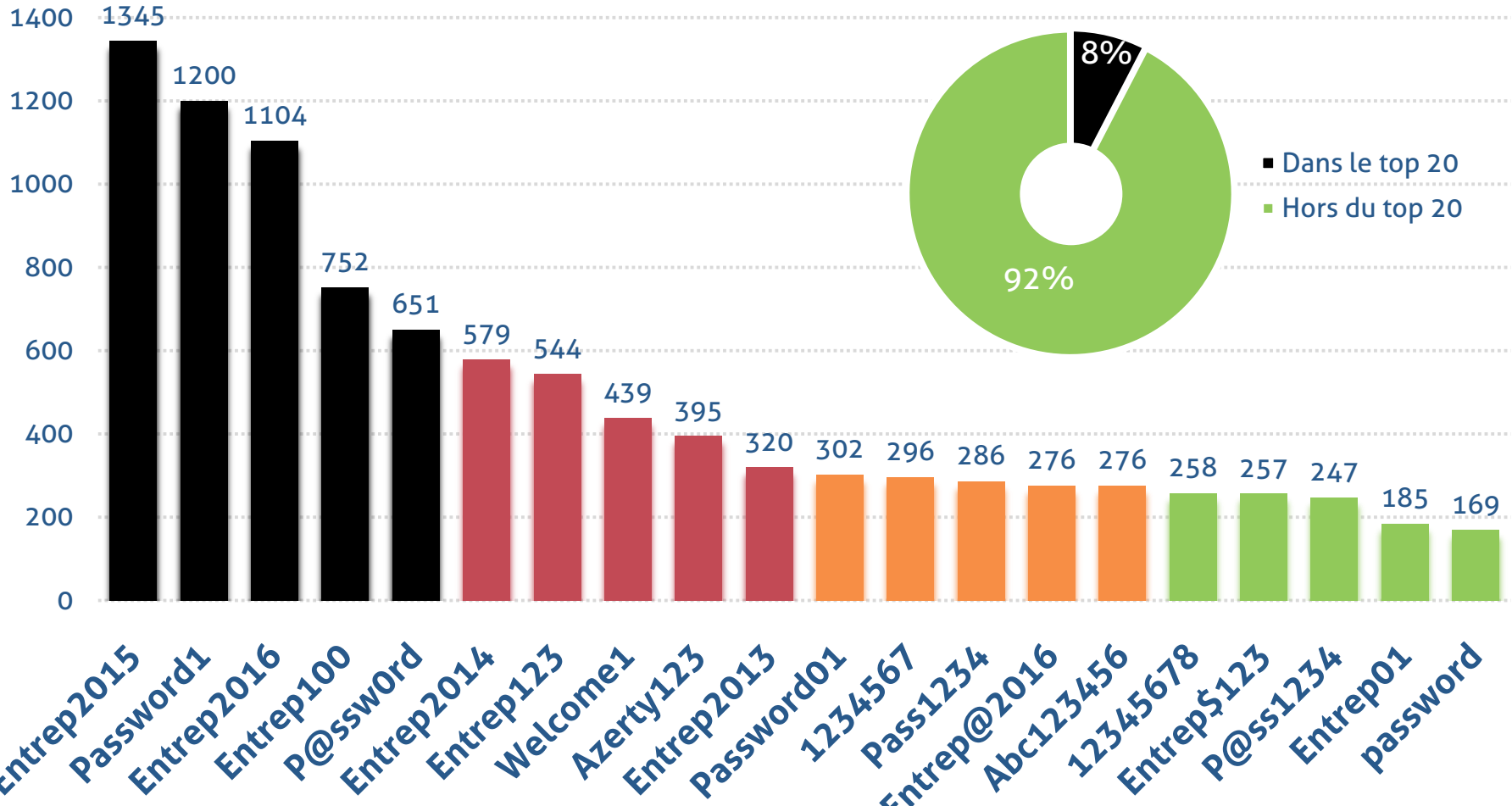
Retours d'expérience

Systèmes d'exploitation plus supportés par Microsoft



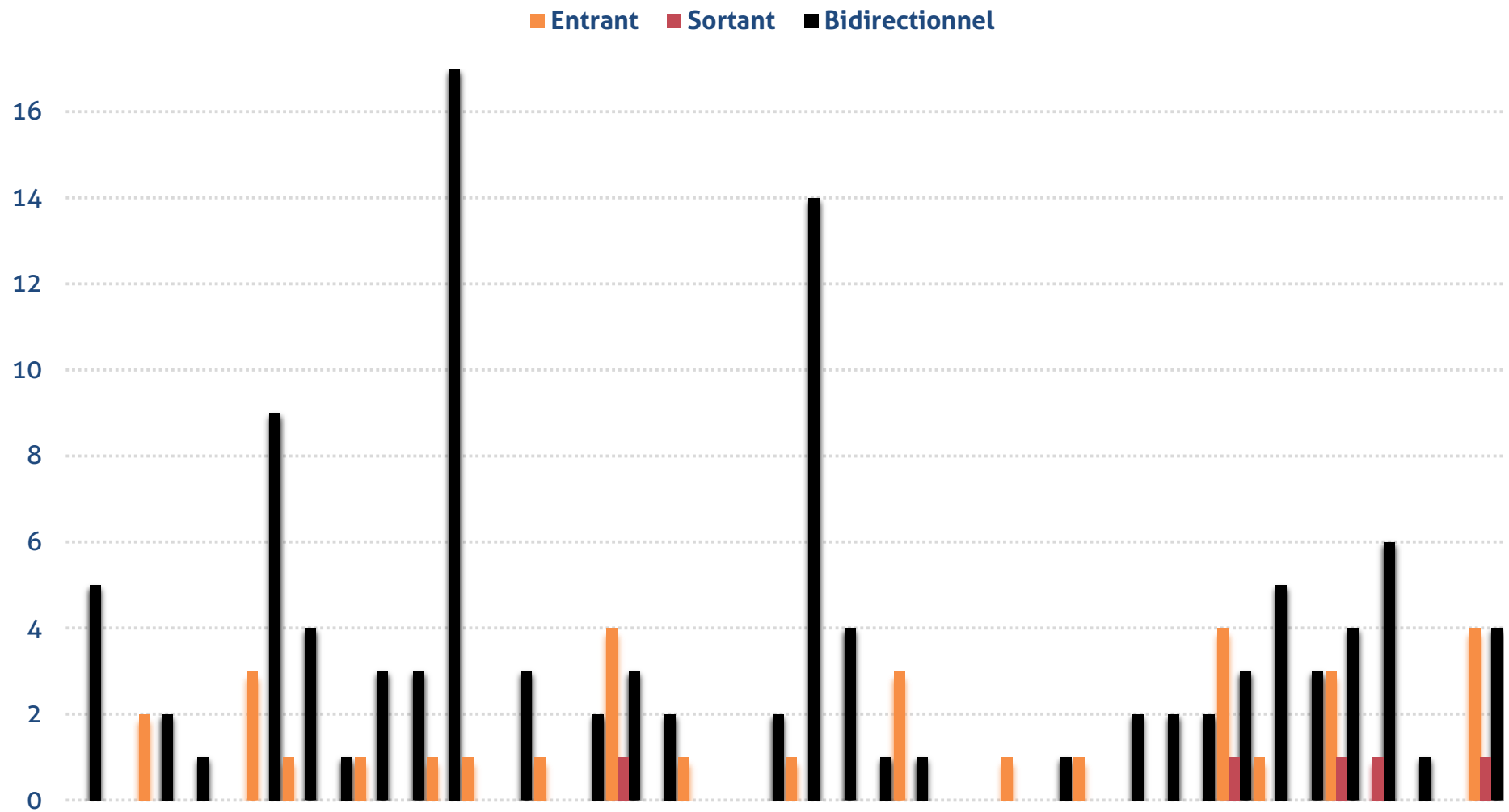
Retours d'expérience

Top 20 des mots de passe, sur 120 000 utilisateurs



Retours d'expérience

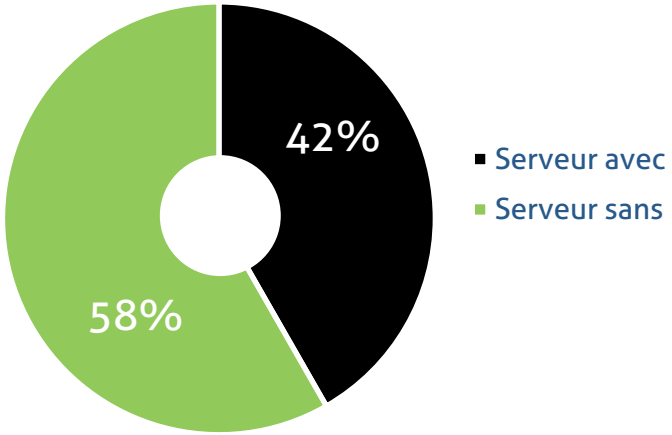
Relations d'approbation externes



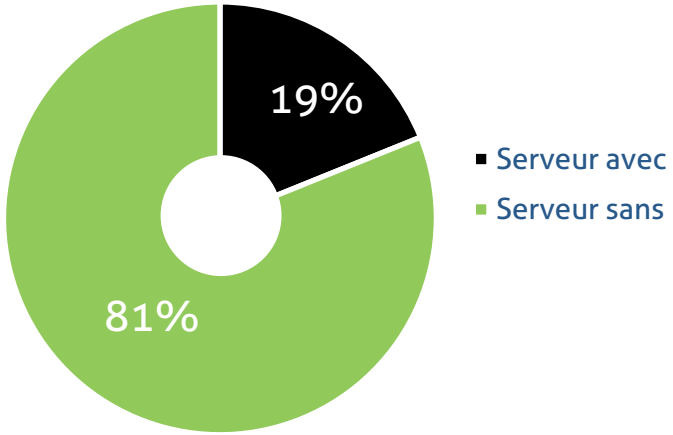
Retours d'expérience

Focus sur un domaine de 1 000 serveurs

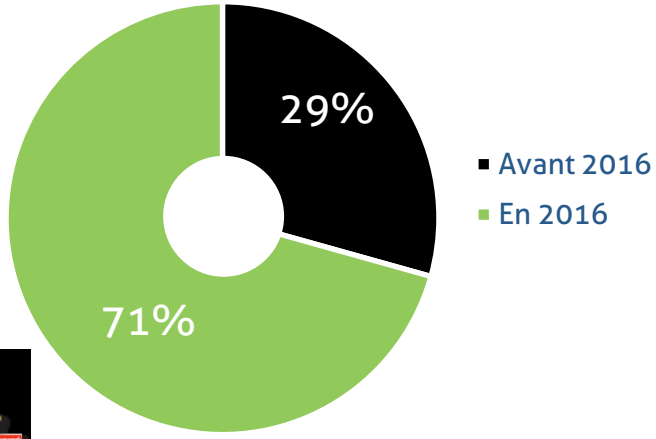
Tâche planifiée possédant un compte administrateur sur 1 autre serveur



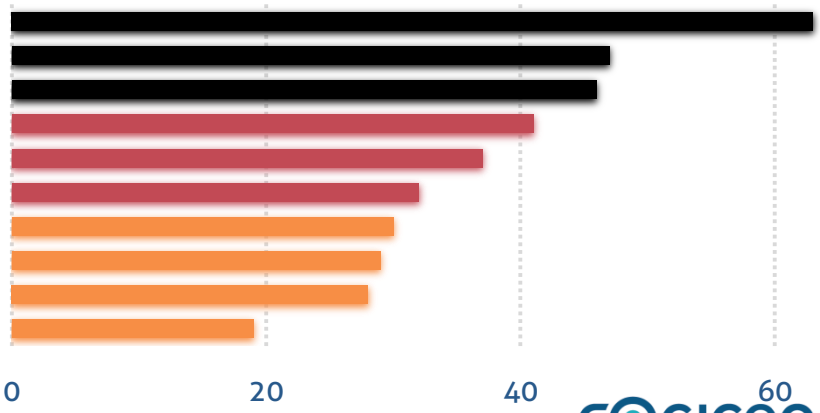
Service possédant un compte administrateur sur 1 autre serveur



Dernière mise à jour de sécurité



Comptes d'administration locaux identiques



Méthodologies de remédiation

Méthodologies de remédiation

Approche

- **Exhaustive**
  - ensemble des objets du domaine
  - ensemble des chemins de compromission
- **Reproductible**
  - mesurer l'évolution du niveau de sécurité
- **Visualisable**
  - via des métriques pertinents
  - regroupés dans un tableau de bord

Méthodologies de remédiation

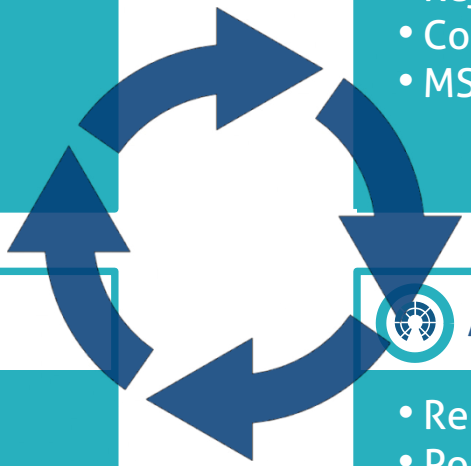
Approche

Comptes utilisateurs

- Domaine et locaux
- Attributs
- Imbrication
- Droits d'administration

Mots de passe

- Top 10
- Rejeu de mots de passe
- Complexité
- MS-Cache



Serveurs

- Version de l'OS
- Services
- Tâches planifiées
- Elévations de privilèges
- Configurations de sécurité
- Correctifs de sécurité

Active Directory

- Relations d'approbation
- Politiques de sécurité de domaine / locales
- Statistiques globales

Ex : Top des serveurs vulnérables

Méthodologies de remédiation

Chantiers

- Migration des serveurs, applications, niveaux fonctionnels
  - Inventaire des applications
  - Décommissionnement des serveurs inutilisés
  - Rationalisation des serveurs non décommissionnables
  - Abandon des protocoles obsolètes
    - Protocoles de nommage secondaires : NBT-NS, LLMNR
    - Protocoles d'authentification : LM, NTLMv1, Wdigest
  - Interdire les connexions distantes pour les comptes locaux
    - SID « LOCAL_ACCOUNT »
    - SID « LOCAL_ACCOUNT_AND_MEMBER_OF_ADMINISTRATORS_GROUP »

- Amélioration du « Patch Management »
  - Mise à jour du processus organisationnel
  - Description des processus techniques

Méthodologies de remédiation

Chantiers

- Outillage de sécurité
  - Revue des privilèges
  - Reporting régulier
    - via PowerShell
  - Outils Microsoft
    - Local Administrator Password Solution (LAPS)
    - Fine-Grained Password Policy
    - Comptes de service administrés (MSA)
    - Groupe « Utilisateurs Protégés »
    - Mode « Administrateur Restreint »
    - Privileged Access Management (PAM)
    - Security Compliance Manager (SCM)
    - Enhanced Mitigation Experience Toolkit (EMET)
    - AppLocker
  - Mise en place d'un système de contrôle automatique
    - Advanced Audit Policy
  - Bastion d'administration

Méthodologies de remédiation

Chantiers

- Gabarits de sécurité
  - Systèmes d'exploitation
  - Systèmes applicatifs
  - Comptes à privilèges
- Politique d'architecture
  - Redécoupage des forêts et des domaines
    - Read-Only Domain Controller (RODC)
  - Règles d'implémentation des relations d'approbation
    - SID Filtering, Selective Authentication
  - VLAN d'administration
- Montée en compétences de sécurité
  - Formation technique des administrateurs
  - Sensibilisations des utilisateurs ayant des privilèges
  - Communication auprès des collaborateurs

Questions ?

Merci pour votre attention.

COGICEO

EXPERTISE TECHNIQUE EN SÉCURITÉ INFORMATIQUE

cogiceo.com

+33(0) 1 85 08 10 70

contact@cogiceo.com

twitter.com/cogiceo

linkedin.com/company/cogiceo