WAVESTONE

Sécurité de l'Active Directory

Les chemins de compromission de l'Active Directory

18/03/2019

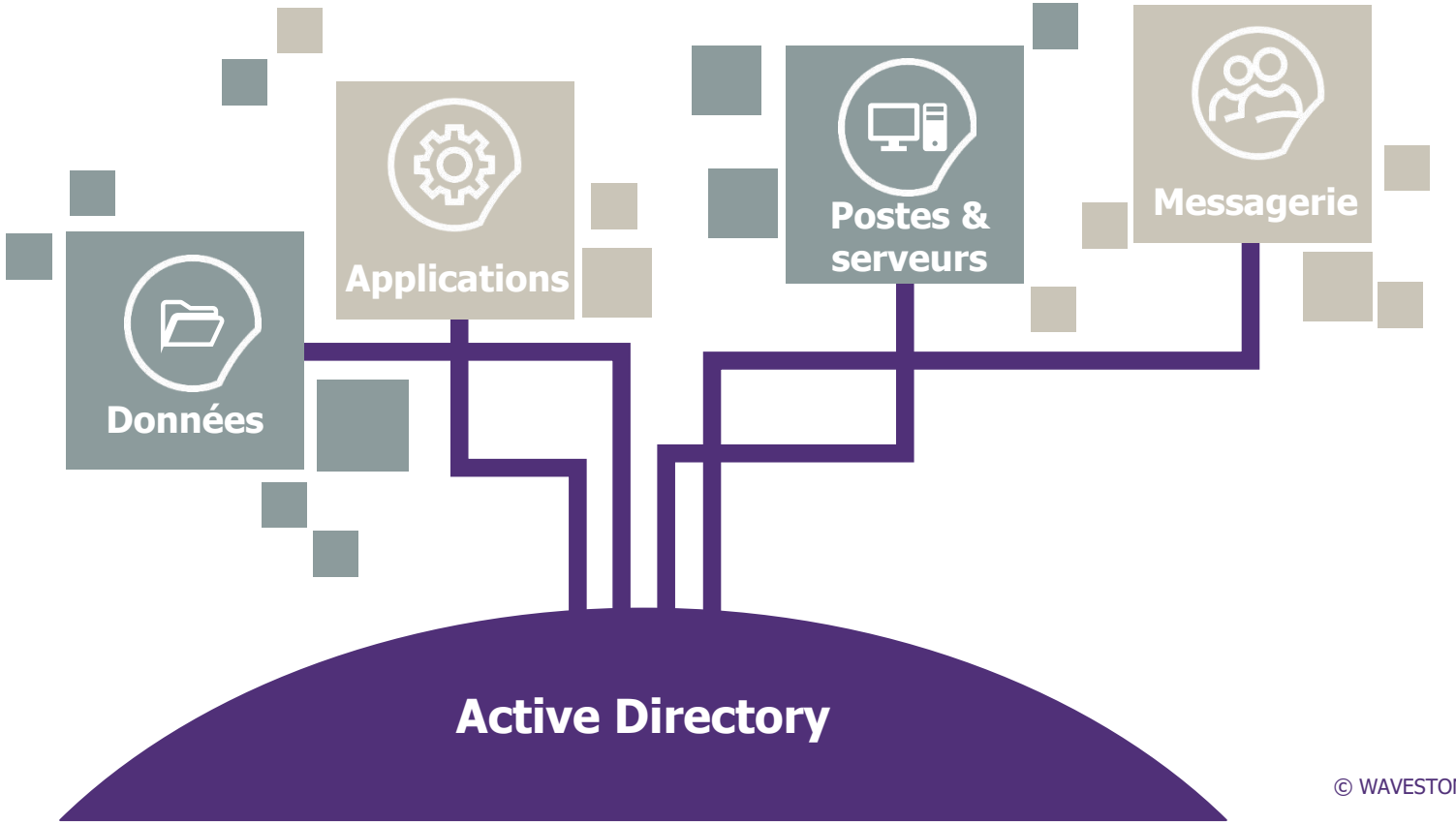
Rémi ESCOURROU
Senior Consultant
remi.escourrou@wavestone.com

@remiescourrou

Cyprien OGER
Senior Consultant
cyprien.oger@wavestone.com

Quel niveau de sécurité pour les systèmes d'information des entreprises ?

Les systèmes d'information reposent sur une **infrastructure centrale**, usuellement Active Directory. Sa compromission permet de prendre le contrôle de l'ensemble **des systèmes et des données** des entreprises.



La quasi-totalité des systèmes d'informations sont vulnérables

Wavestone a réalisé sur 2017 et 2018, des tests d'intrusion sur 25 systèmes d'information de grandes entreprises.

96% se sont soldés par la **compromission totale de l'Active Directory**

Quels chemins pour compromettre le SI ?

Ciblage d'un premier serveur

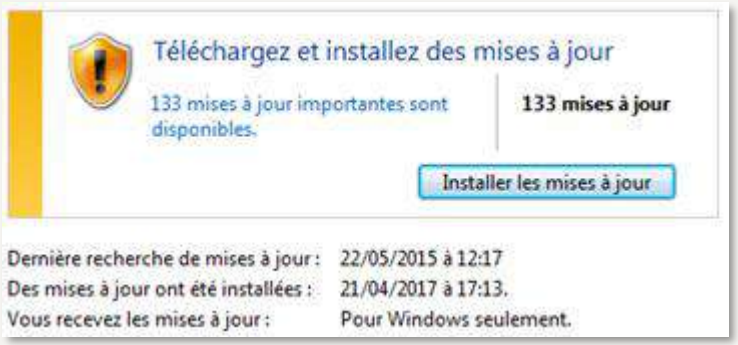
Présence d'une vulnérabilité pour laquelle un correctif de sécurité a déjà été publié.

75 % d'un défaut de mise à jour

Réseau interne

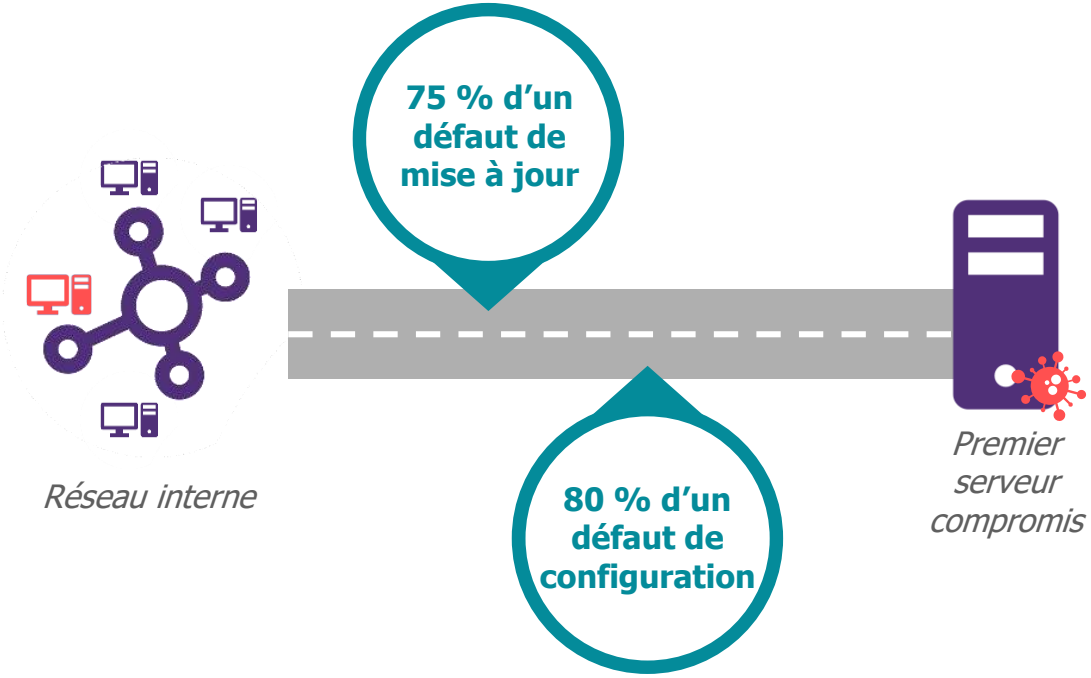
Premier serveur compromis

Actuellement dans votre SI :



Quels chemins pour compromettre le SI ?

Ciblage d'un premier serveur

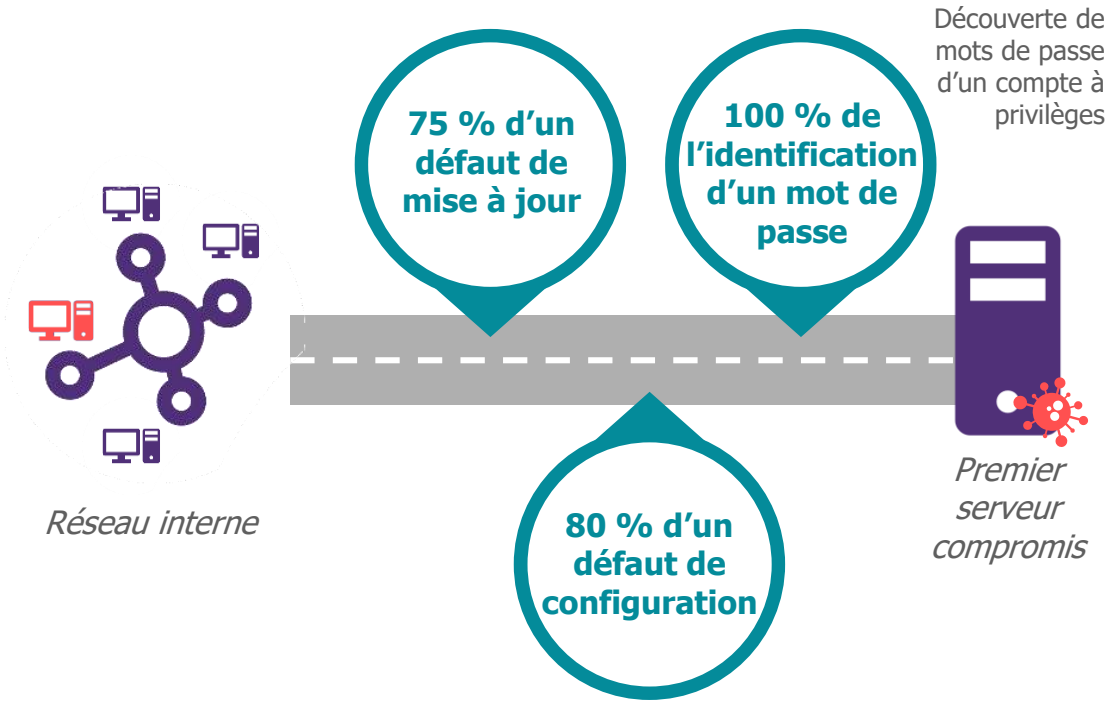


Présence d'un défaut de configuration (mot de passe par défaut, absence d'authentification, etc.)

Actuellement dans votre SI :

Quels chemins pour compromettre le SI ?

Ciblage d'un premier serveur



Actuellement dans votre SI :

```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Pa

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName
```

```
PS C:\                                > Invoke-CleverSpray -Passw
-DomainController
[!] Current lockout threshold is 5
[!] Only users having 'badpwdcount' attribute lower than
[+] Old password detected: M[redacted]2017!
[+] Old password detected: p[redacted]2017!
[+] Old password detected: m[redacted]2017!
[+] Old password detected: m[redacted]2017!
[+] Success:   Tr[redacted]2017!
[+] Old password detected: S[redacted]2017!
[+] Old password detected: p[redacted]2017!
[+] Success:   M[redacted]2017!
[+] Old password detected: O[redacted]2017
[+] Old password detected: W[redacted]20
[+] Success:   C[redacted]2017!
[+] Old password detected: N[redacted]20
```

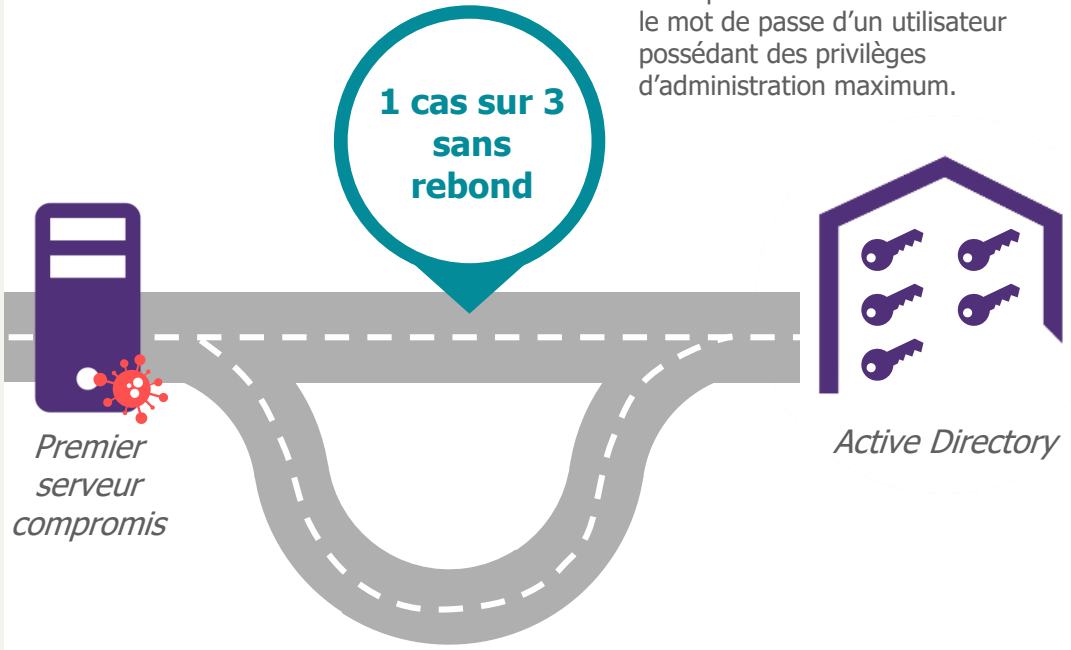
Quels chemins pour compromettre le SI ?

Actuellement dans votre SI :


```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1607
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
        tspkg :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        wdigest :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        kerberos :
         * Username : svc-SQLDBEngine01
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAGoodPassword99!
        ssp :
        credman :
```

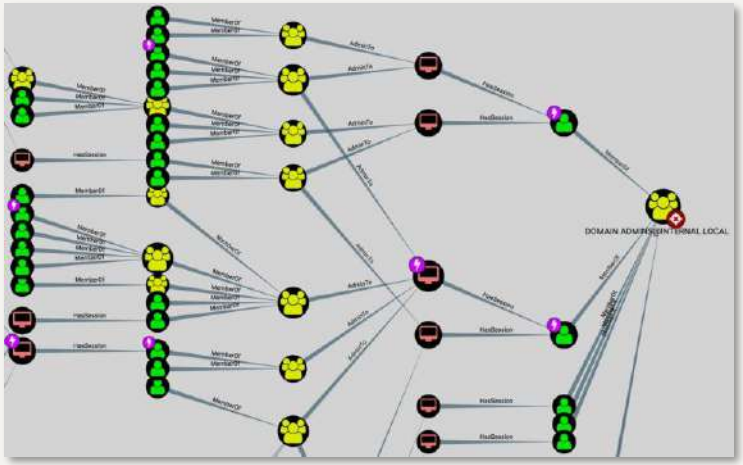
Compromission totale

Il est possible d'extraire en mémoire le mot de passe d'un utilisateur possédant des privilèges d'administration maximum.

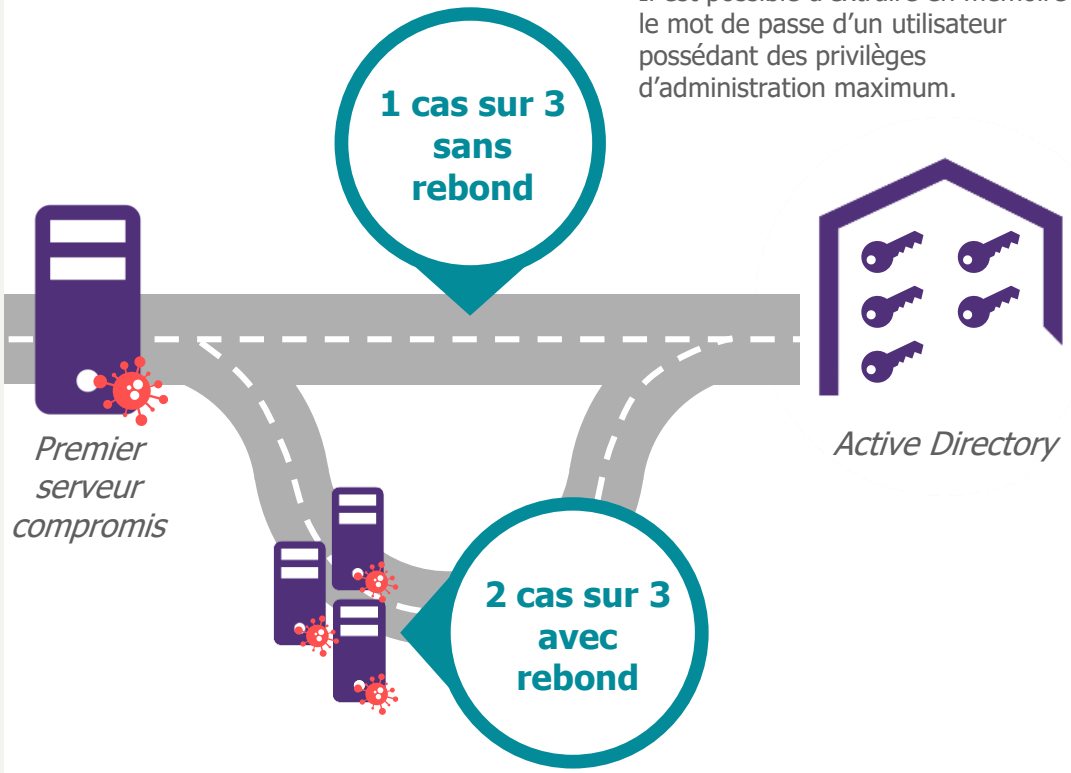


Quels chemins pour compromettre le SI ?

Actuellement dans votre SI :



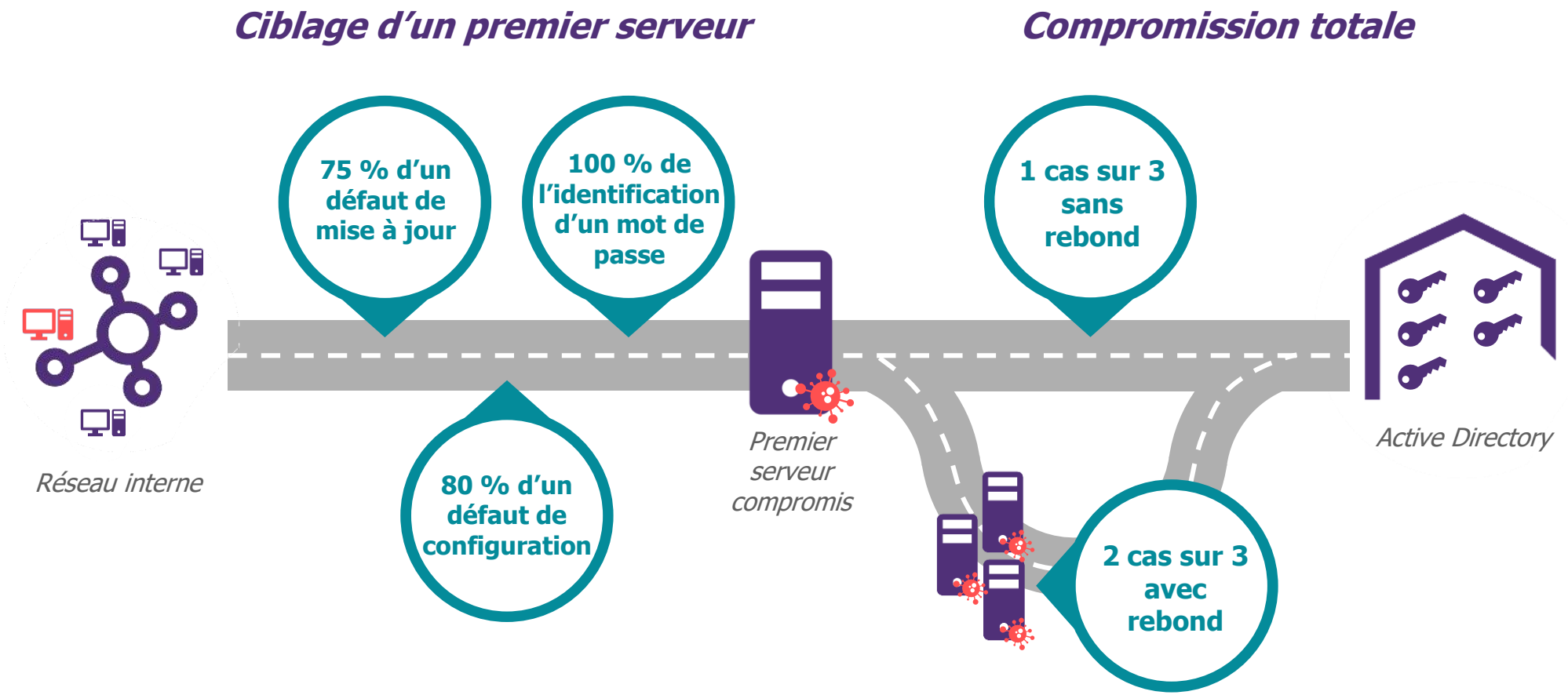
Compromission totale



Il est possible d'extraire en mémoire le mot de passe d'un utilisateur possédant des privilèges d'administration maximum.

Plusieurs compromissions successives sont nécessaires pour récupérer des privilèges maximum.

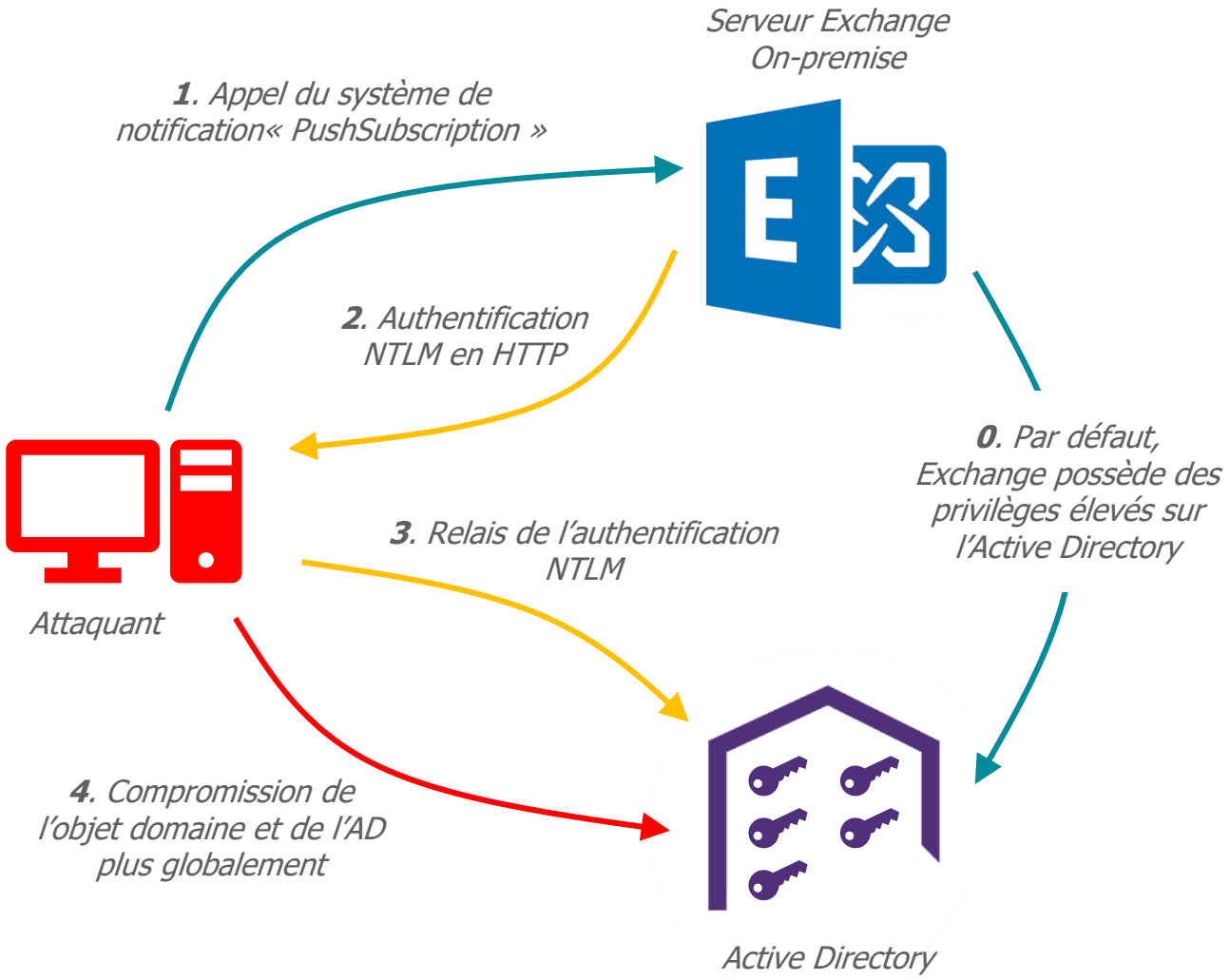
Quels chemins pour compromettre le SI ?



Dans 80 % des audits réalisés, la compromission est totale en moins de 24h

BREAKING NEWS

ONE API CALL AWAY FROM DOMAIN ADMIN THANKS TO EXCHANGE



Remédiation

Déployer les mises à jour cumulatives d'Exchange :

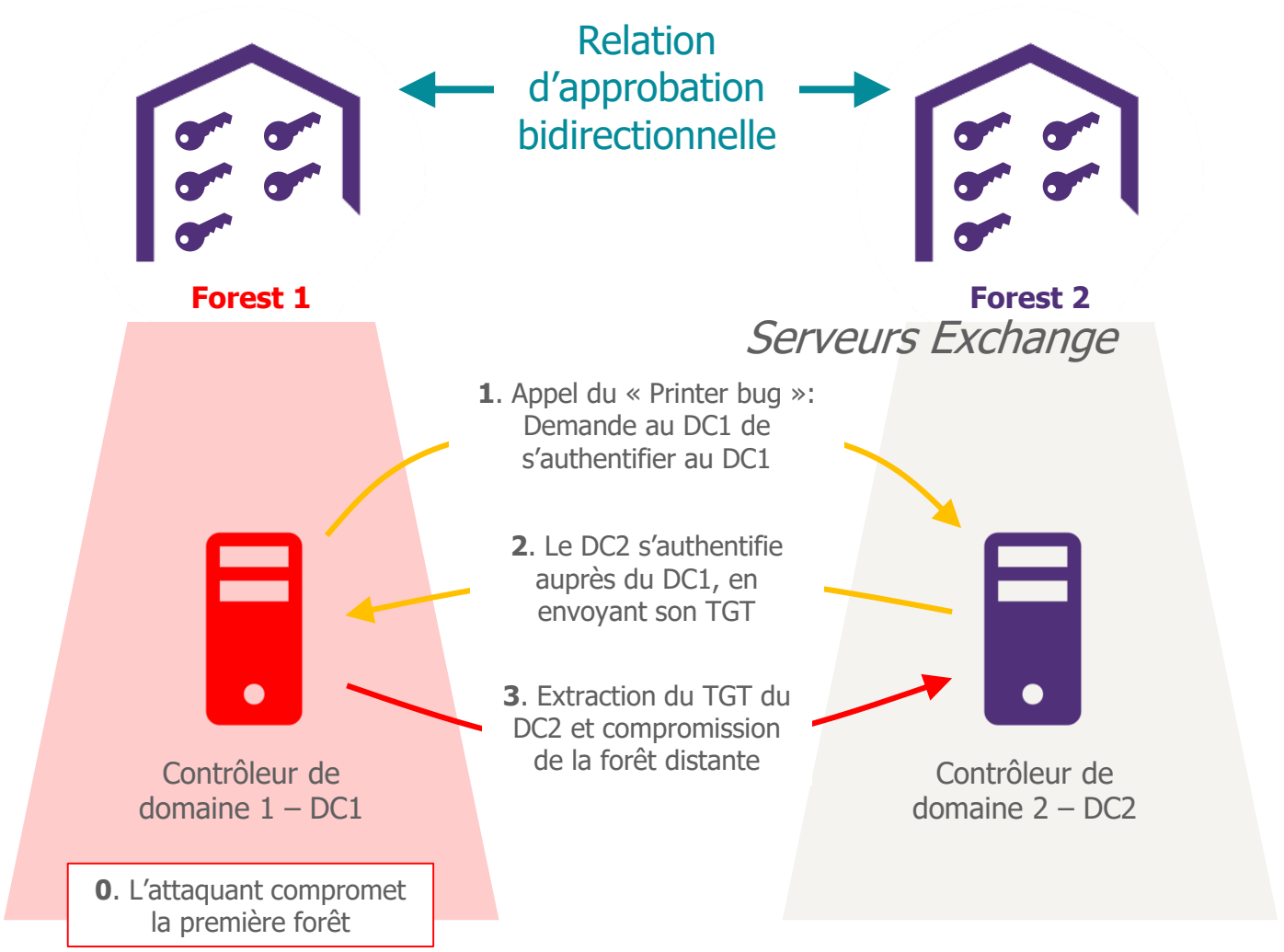
Exchange Server 2019 : CU1
Exchange Server 2016: CU12
Exchange Server 2013 : CU22
Exchange Server 2010 : Rollup 26

Corriger les ACE Exchange à la racine du domaine (voir KB 4490059)

@_dirkjan
https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

BREAKING NEWS

NOT A SECURITY BOUNDARY: BREAKING FOREST TRUSTS



Remédiation

Désactiver le « Spooler » d'impression sur :

Contrôleurs de domaine
Serveurs Exchange
Serveurs sensibles (WSUS, SCCM)

Etudier la possibilité d'interdire la délégation de TGT à travers les relations d'approbation

@harmj0y
https://posts.specterops.io/not-a-security-boundary-breaking-forest-trusts-cd125829518d

Merci de votre attention !

WAVESTONE

Rémi ESCOURROU
Senior consultant

M +33 (0)7 62 62 51 02
remi.escourrou@wavestone.com

Cyprien OGER
Senior consultant

M +33 (0)6 98 78 64 72
cyprien.oger@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_