SOPHOS

Panorama des techniques de résistance aux antivirus (anti-AV)

OSSIR - JSSI 2004

4 Mai 2004

Vanja Svajcer, Principal Virus Researcher

vanja.svajcer@sophos.com

Introduction

SOPHOS

- Contexte
- Techniques anti-AV
- Stratégies de protection
- Le futur

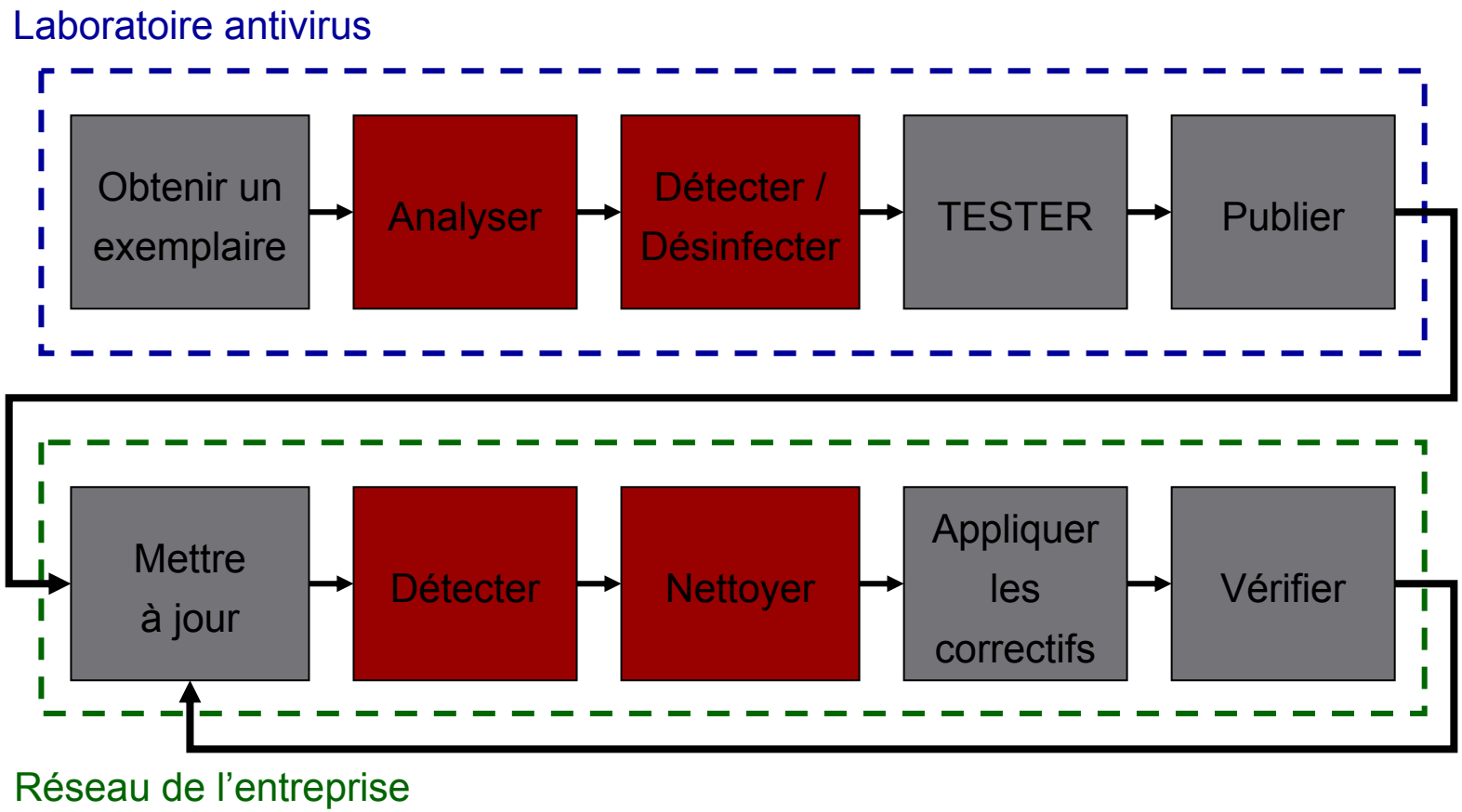
Techniques anti-AV

SOPHOS

Ensemble de méthodes et d'outils utilisés par les créateurs de virus pour contrer, retarder ou désactiver le processus de protection antivirus

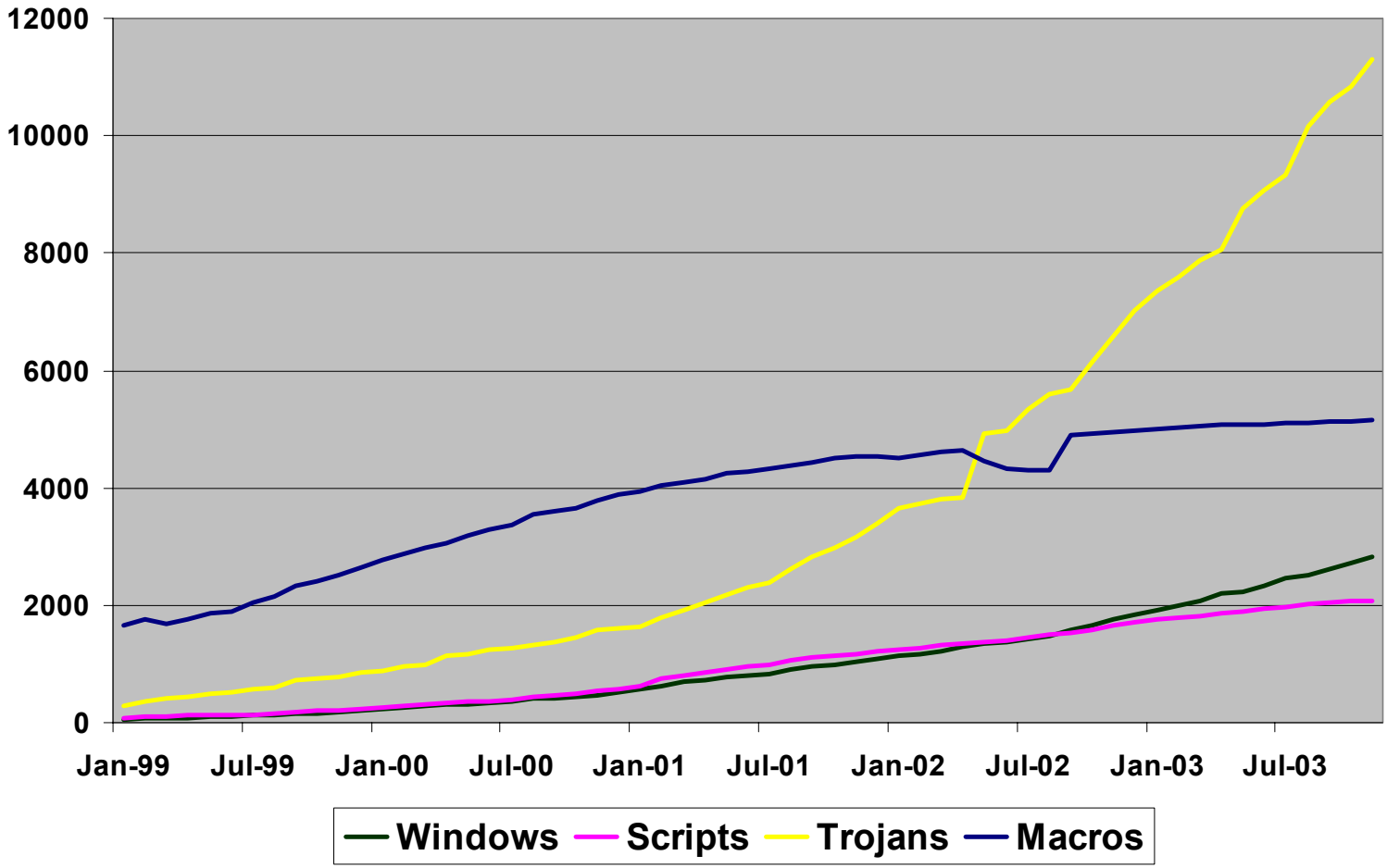
Processus de protection contre les virus

SOPHOS



Principaux types de codes malicieux

SOPHOS



La menace actuelle – virus typiques du 21ème siècle

SOPHOS

- Le sens de la vie
  - Accès au système de la victime
  - Sécurité du système d'exploitation compromise
  - Keylogging
  - Portes dérobées
  - Dénis de services distribués "esclaves"
  - Relais pour le spam
  - Piratage

Techniques Anti-AV

SOPHOS

- Anti-analyse
- Anti-détection
- Anti-nettoyage

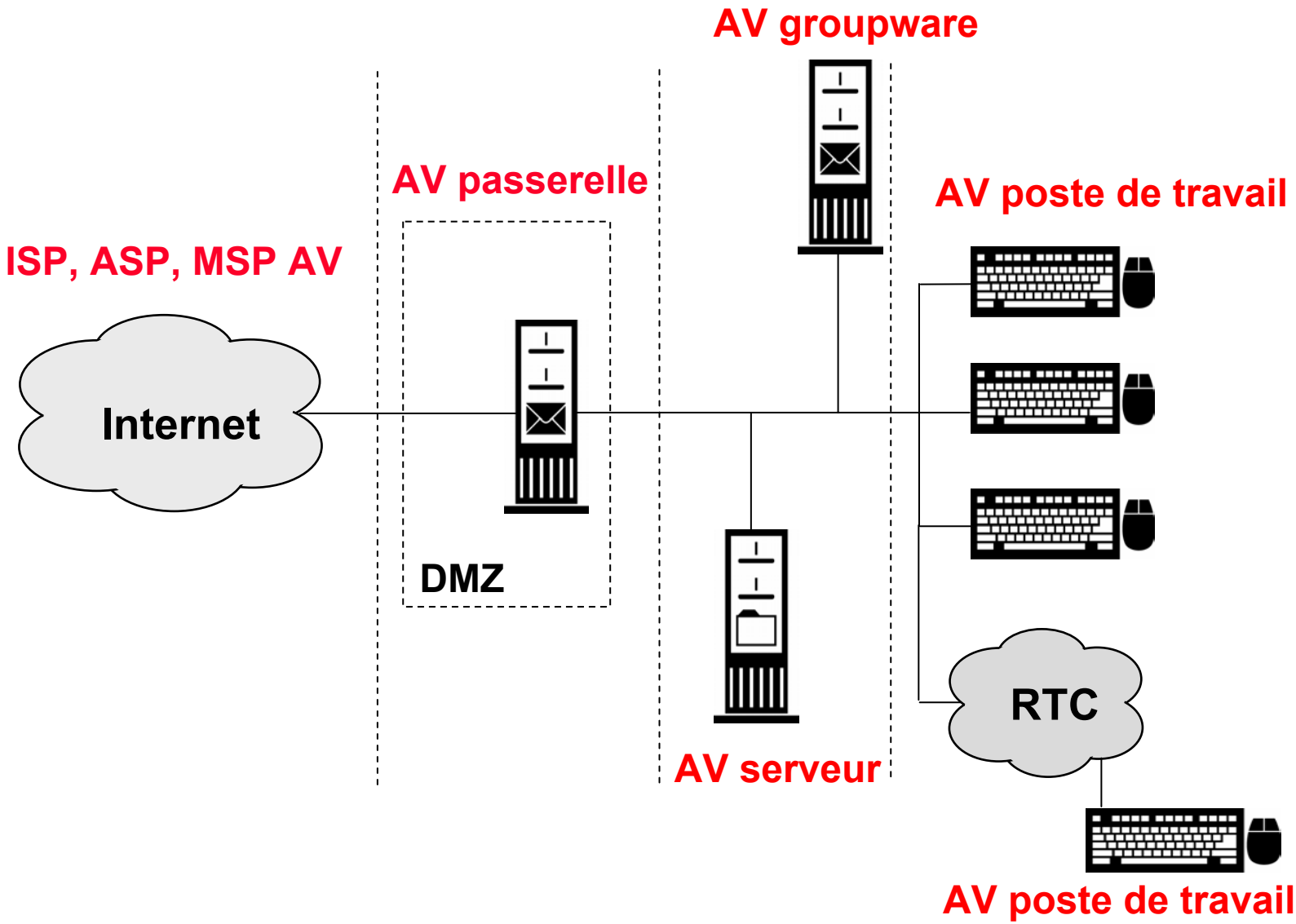
Techniques anti-analyse

SOPHOS

- Anti-débogage
- “Run-time packers”
- Chiffrement
- Polymorphisme

Déploiement antivirus – approche multi-niveau

SOPHOS



Techniques anti-détection (poste de travail)

SOPHOS

- Polymorphisme
- Furtivité (dissimulation)
- Packers
- Désactivation des antivirus et autres applications de sécurité
- Autres (NTFS, utilisant des applications légitimes)

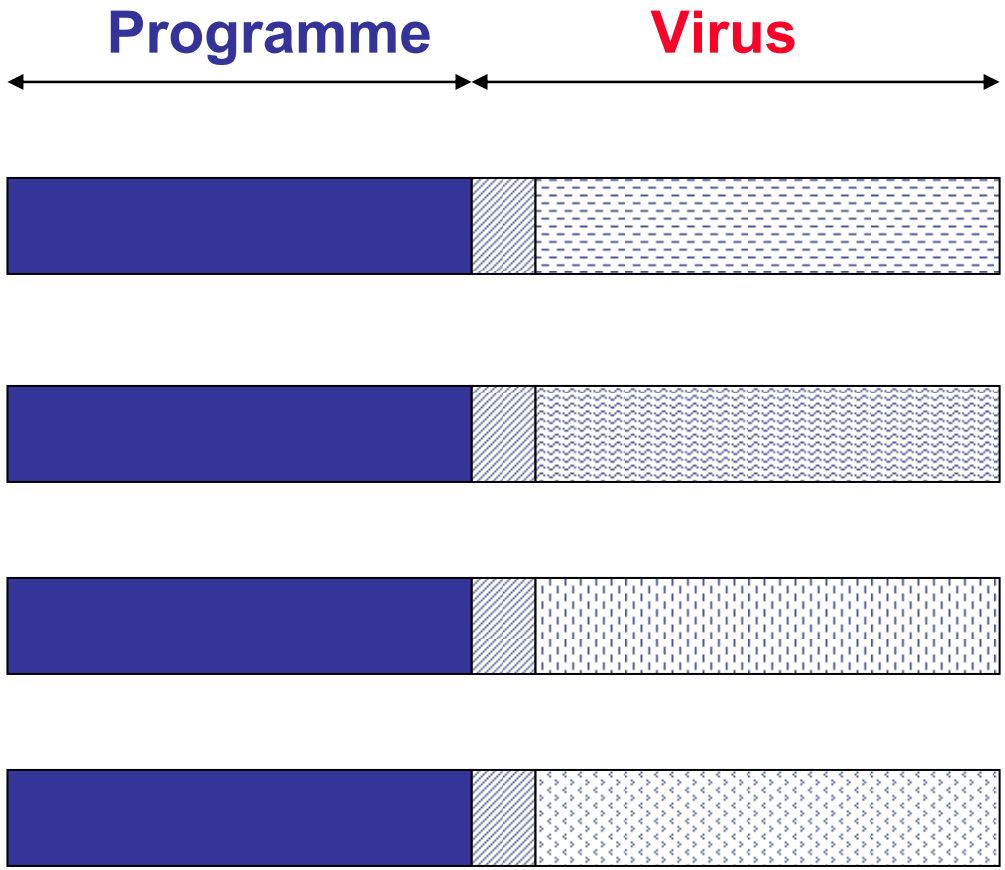
Dissimulation dans les fichiers

SOPHOS

- Les virus se contentaient de simplement ajouter leurs codes à des fichiers exécutables
- Les scanners pouvaient alors rechercher des séquences fixes d'octets pour identifier le virus
- Les créateurs de virus se mirent alors à chiffrer le code viral, pour ne le déchiffer qu'à l'exécution du programme

Virus chiffré

SOPHOS



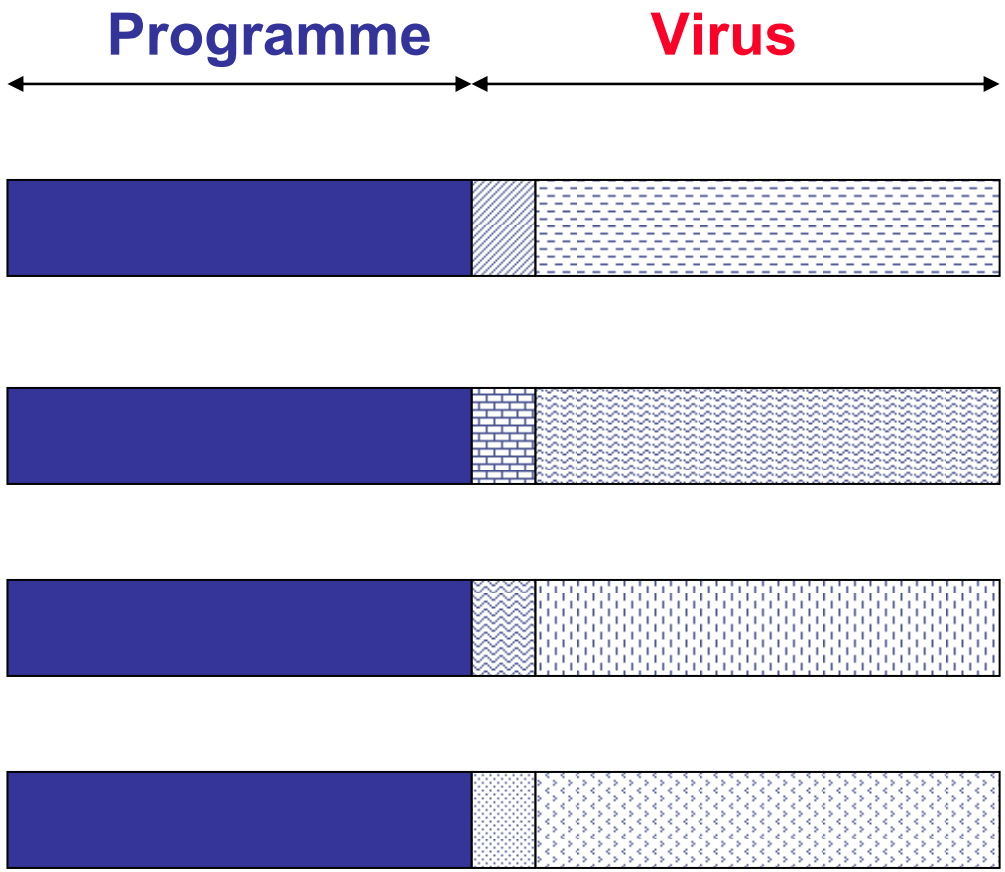
Dissimulation renforcée

SOPHOS

- Un chiffrement simple n’est pas suffisant
- Avec le polymorphisme, le code de chiffrement varie à chaque nouvelle infection
- Il n’y a plus de boucle de déchiffrement “fixe” à détecter

Virus polymorphiques

SOPHOS



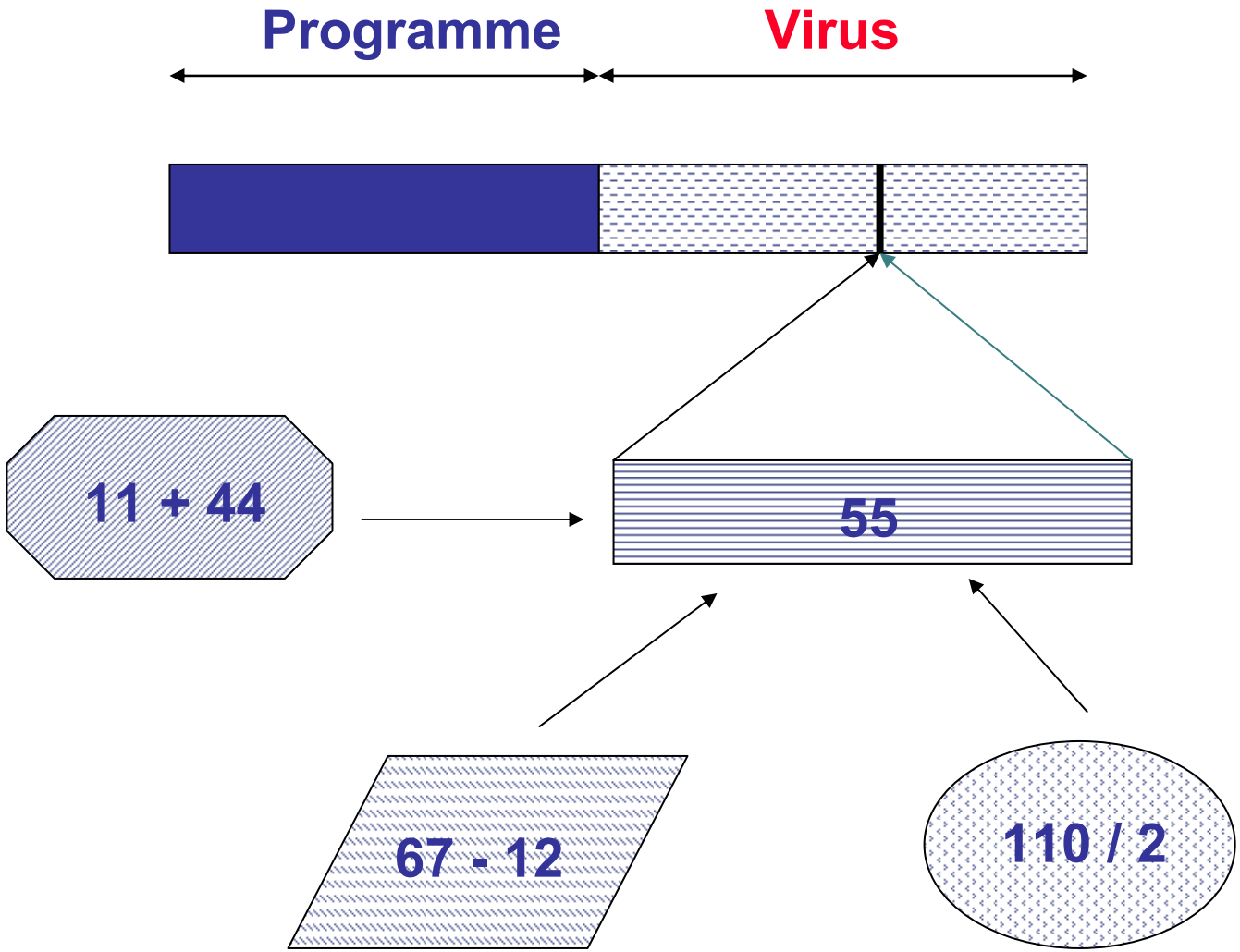
Virus métamorphiques

SOPHOS

- Change les instructions utilisées dans le corps du virus
- Ajoute éventuellement des instructions sans action
- Scinde éventuellement les instruction en deux étapes ou plus, produisant le même résultat
- Combine éventuellement des instructions
- Il n’y a pas de boucle de déchiffrement

Virus métamorphique

SOPHOS



La solution est … un émulateur

SOPHOS

- La plupart des scanners incluent maintenant un émulateur
- Il s'agit d'une simple boucle:
  - Lit les octets de code
  - Décode ces octets
  - Exécute les instructions décodées
  - Observe s'il y a une écriture en mémoire
  - Traite l'instruction suivante

Que fait-il ?

SOPHOS

- L’émulateur observe le déchiffrement du virus polymorphique au fur et à mesure de son écriture en mémoire
- Dans la plupart des cas, il lui suffit de déchiffrer une partie du corps du virus pour le reconnaître
- Le corps du virus ainsi déchiffré est ensuite analysé par le scanner

Astuces anti-émulateurs

SOPHOS

- Les créateurs de virus essaient de faire échec aux émulateurs:
  - Appels aux fonctions API système
  - Boucles qui ne font rien
  - Instructions bidons (“junk”)
  - Utilisation de la gestion structurée des exceptions
  - Exécution aléatoire du code viral
  - Vérification du temps écoulé
- Les émulateurs doivent évoluer
  au fur et à mesure que les créateurs de virus mettent au point de nouvelles astuces

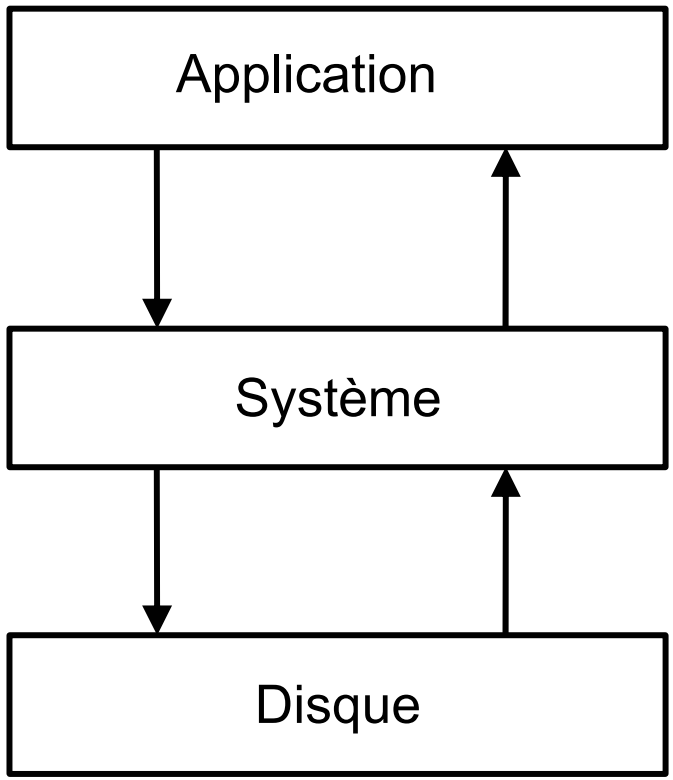
Techniques de dissimulation (furtivité)

SOPHOS

- Une fois actif en mémoire, un virus peut dissimuler:
  - Fichiers
  - Process
  - Clés de registres
  - Ports
  - Mémoire
  - Descripteurs d'objets ("Object handles")

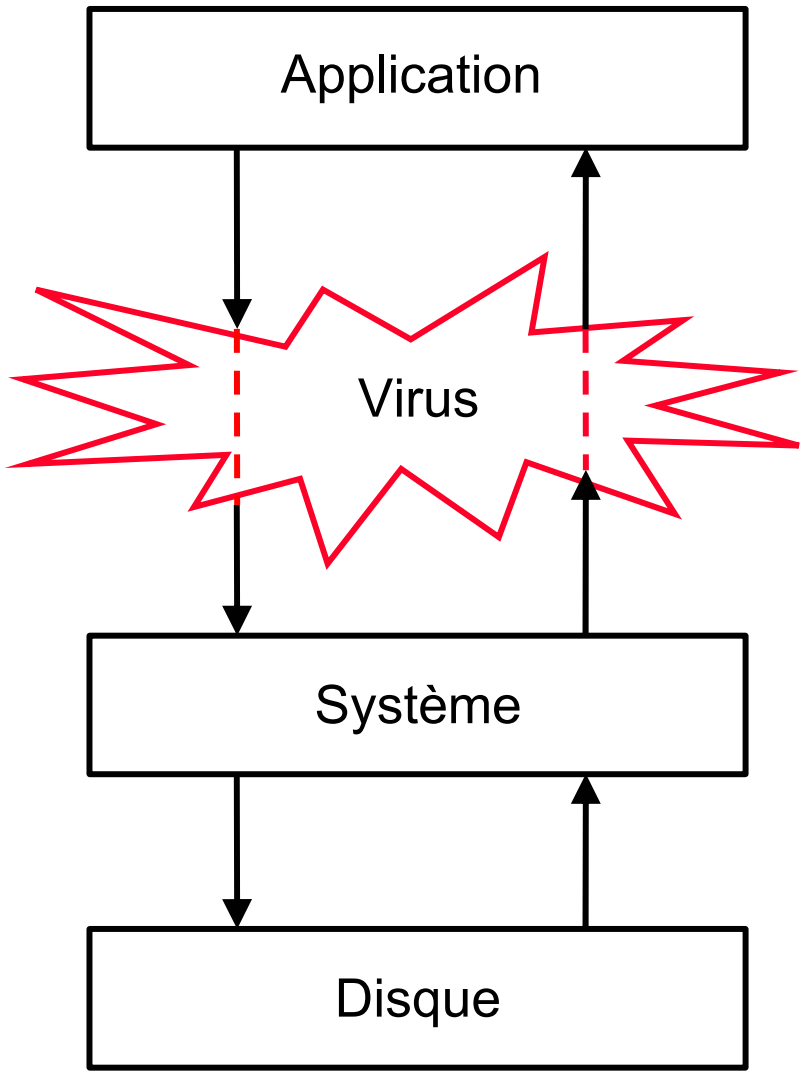
Système normal

SOPHOS

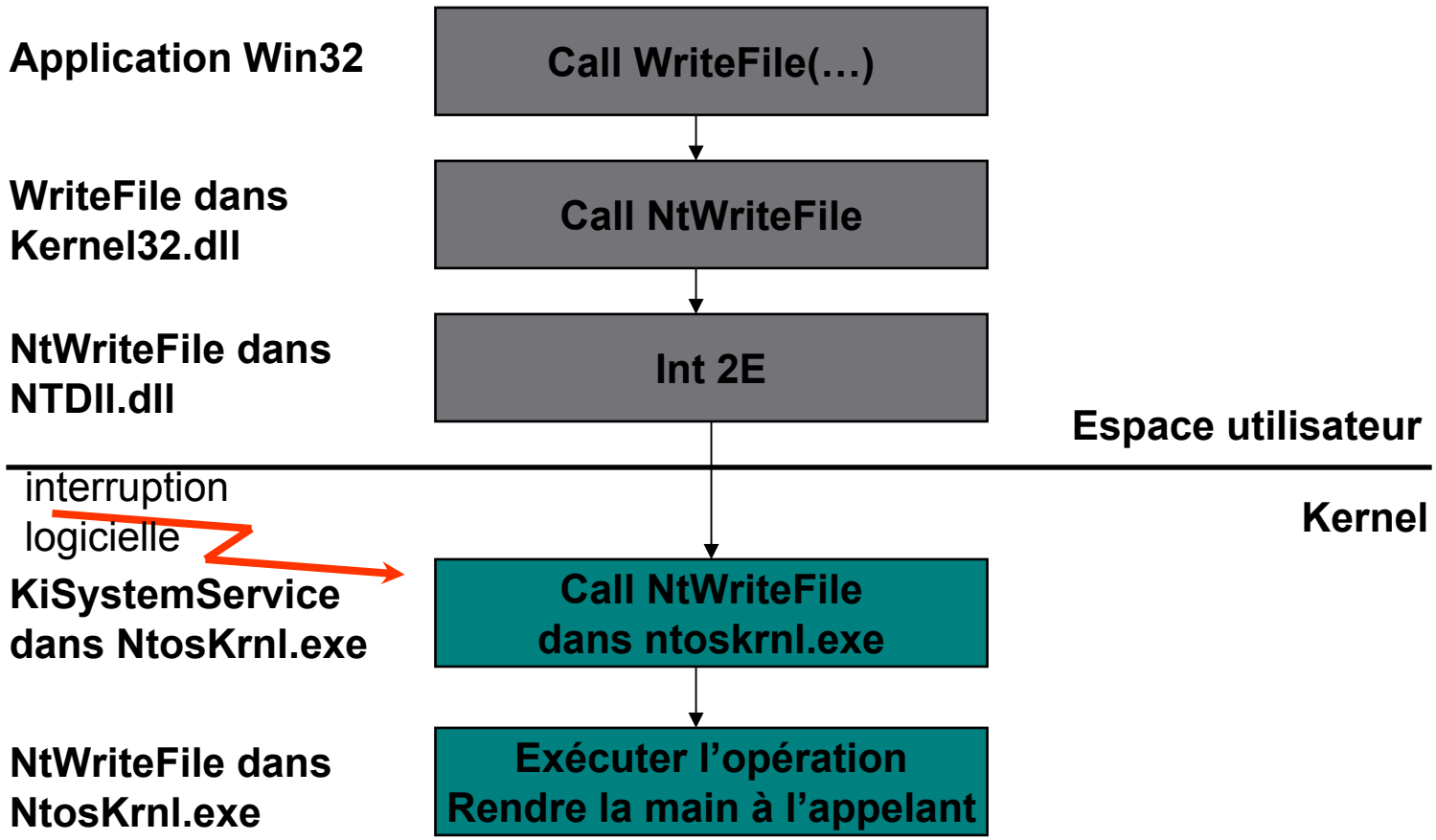


Virus installé

SOPHOS



Appel aux services systèmes Windows



Interception (“Hooking”)

SOPHOS

- Mode utilisateur
  - kernel32.dll
  - advapi32.dll
  - ws2_32.dll
  - user32.dll
  - ntdll.dll

Hooking (Hacker Defender)

SOPHOS

- Pour chaque (nouveau) process du système:
  - Charger le code d'interruption
  - Trouver les fonctions exportées à intercepter
  - Sauvegarder l'offset de la fonction interceptée
  - Sauvegarder les premiers x octets de la fonction
  - Modifier le point de départ de la fonction avec le saut

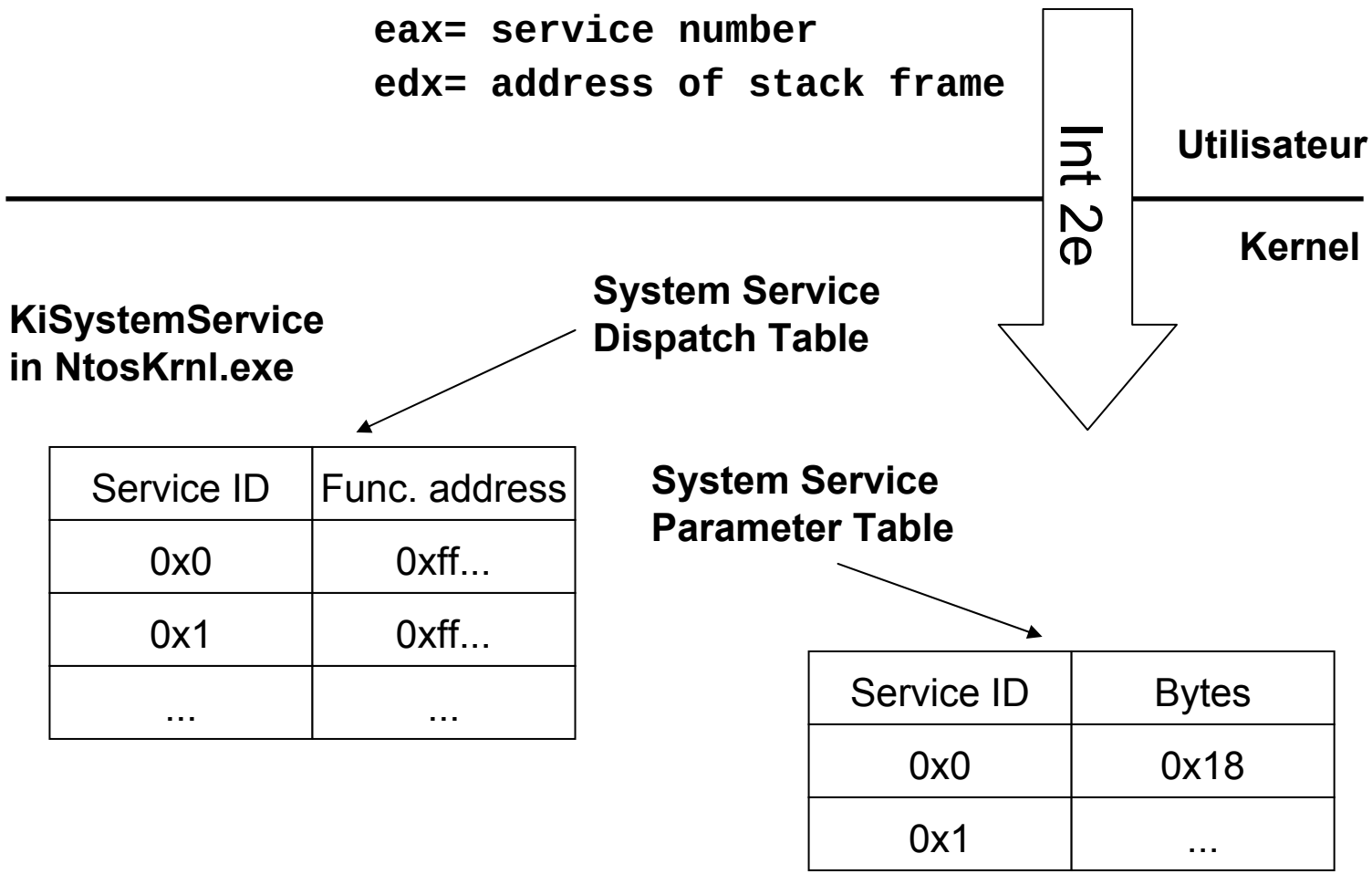
Hooking (Hacker Defender)

SOPHOS

- Quand la fonction interceptée est appelée
  - Appeler la fonction d'origine
  - Modifier les résultats
  - Repointer vers la fonction interceptée
  - Retourner les résultats modifiés

KiSystemService handler

SOPHOS



Service ID	Func. address
0x0	0xff...
0x1	0xff...
...	...

Service ID	Bytes
0x0	0x18
0x1	...

Hooking

SOPHOS

- Mode Kernel
  - Intercepte int 2e
  - Change SSDT
  - Crée un pseudo-driver en mode kernel
  - Ou ajoute un nouveau service système
  - Et intercepte les exports ntoskrnl.exe

Hooking - ierk8243

SOPHOS

- NtOpenKey
- NtCreateKey
- NtEnumerateKey
- NtCreateFile
- NtOpenFile
- NtDeviceIoControl
- NtQueryDirectoryFile
- NtQuerySystemInformation
- PsSetCreateProcessNotifyRoutine

Run-time packers

SOPHOS

- UPX, ASPack, FSG, Petite
  - Des “packers” sont utilisés sur le même fichier
  - Rend le “reverse engineering” plus difficile
  - Les “packers” utilisent des techniques d’anti-débogage
  - Les scanners peuvent ne pas détecter les virus “repackagés”

Techniques anti-détection (passerelle)

SOPHOS

- Messages MIME mal formés
- Obscurcissement MIME (“MIME obfuscation”)
- Chiffrement (W32/Bagle-Zip)
- Pièces jointes compressées (avec mot de passe)

Obscurcissement MIME (“MIME obfuscation”)

SOPHOS

```
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary=WIFVHABY

--WIFVHABY

This is just a test message

--WIFVHABY
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable

<IFRAME SRC=3DCID:EMAIL WIDTH=3D0>
--WIFVHABY
Content-Type: audio/x-ms-wax;
 name=email.com
Content-Transfer-Encoding: base64
Content-ID: <EMAIL>

[base64 encoded file]
--WIFVHABY
--
```

Obscurcissement MIME ("MIME obfuscation")

SOPHOS

```
MIMe-vERSioN: 1(*T).0
COntEnT-TyPe: (<!)mU(3)l(/)TIp(*)aRT(!)/M(;)i(^)X(eCz)E(/`x)d;
 (,#?)Bo(8l)uN(_)Da(*F)Ry=WIFVHABY

XXEMEDWSIUKZTCJYCBTCRRBYFLUICTWOURLFJDDRB
WIFVHABY--
--WIFVHABY
This is just a test

--WIFVHABY
coNTent-TYPE: (6{)t(=`)e(x-1)xt(bU)/hT(w)ML
coNtEnT-TRANSFEr-ENCoDING: Qu(ZYT)OT(0&y)E(DBZ)d(a)-
(_)PRi(p9Q)N(|N)TaBlE

=3CIF=52A=4DE =53RC=3D=43I=44=3A=45MAIL =57=49=44T=48=3D=30=3E
--WIFVHABY
ConTeNt-TYpe: (~S)A(I8t)U(w)D(y:,)Io/(JP)x-M(,)s-w(J)A(+)X(8);
 (')Nam(|lz)E(oJ_)=(M#g)e(NO>)m(J)a(6U)il(b#).c(lp')o(Eh)M
ConTenT-tRaNSFER-eNCoDiNG: bA(@h)se(*)64
coNtENt-iD: <(wFe)EM(gq6)ai(*)L>

[base64 encoded file]
--WIFVHABY
OIALNKVLKBDYHURLTQQGRACSXCSGLWKJVSDROSQBJOXYMYAFRFQJGKA
----
```

Techniques anti-nettoyage

SOPHOS

- Furtivité
- File locking
- Surveillance de process
- Surveillance de la base de registres
- NTFS ADS

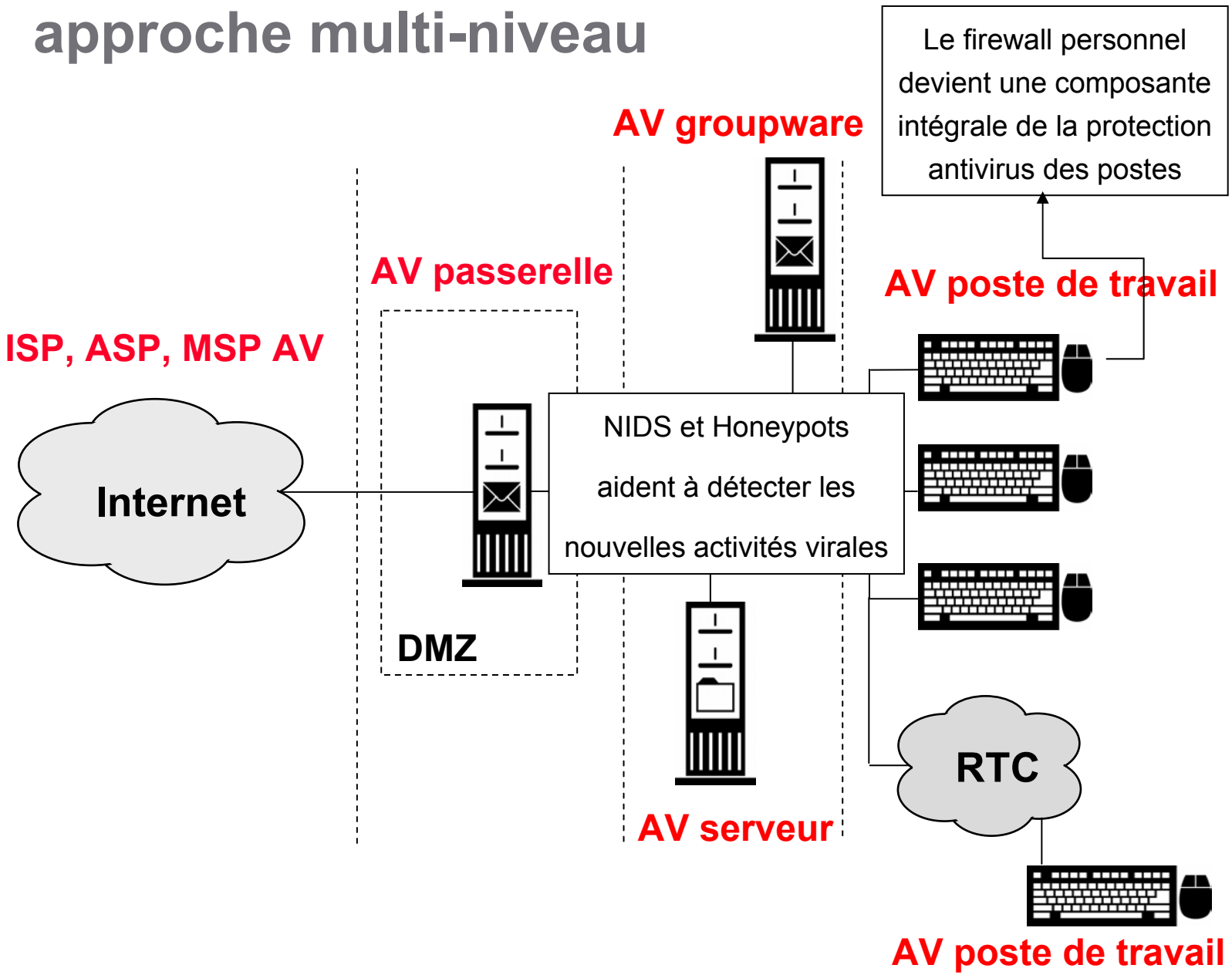
Stratégie de protection

SOPHOS

- Le logiciel antivirus est seulement un outils parmi d'autres
- IDS
- Firewall
- Firewall personnel
- Gestion des correctifs de sécurité ("patchs")
- Topologie réseau

Déploiement antivirus – approche multi-niveau

SOPHOS



Stratégies de protection

SOPHOS

- Procédures et politiques
- Equipes de gestion de crises
  (“Emergency Response Teams”)
- Education

Le futur

SOPHOS

- Améliorer le scan de la mémoire
- Intégrer la détection des virus furtifs dans les logiciels antivirus
- Ne plus vérifier uniquement les fichiers contre le code malicieux
- De plus en plus de virus utiliseront furtivité et polymorphisme

Questions - Réponses

SOPHOS