



ExeFilter & BlindFTP

(SSTIC06 suite)

SSTIC 2008 rump sessions – <http://www.sstic.org>

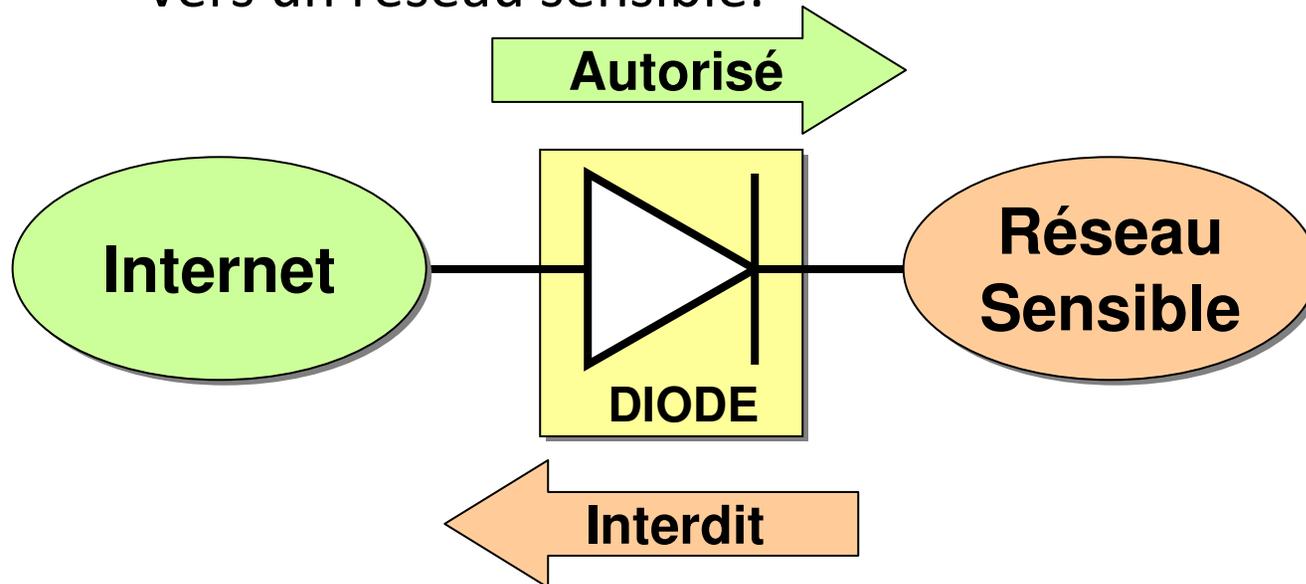
Philippe Lagadec – NATO/NC3A
philippe.lagadec(à)nc3a.nato.int

Rappel: Diode réseau & ExeFilter

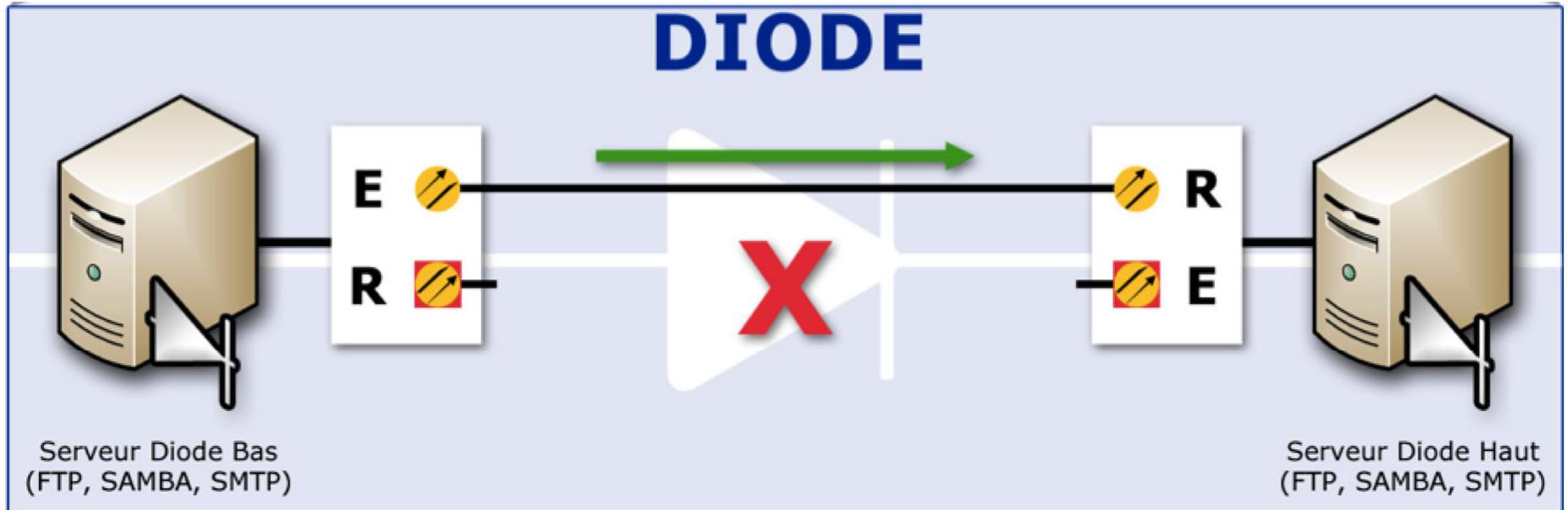
- Présentation à SSTIC06: <http://www.decalage.info/sstic06>
- 2 projets du CELAR pour bâtir des **interconnexions sécurisées** entre un réseau sensible et un réseau de confiance moindre (i.e. Internet)
- **Diode réseau (+BlindFTP):**
 - Pour garantir des transferts unidirectionnels de données.
 - Réseau bas => Réseau Haut uniquement
- **ExeFilter:**
 - Pour filtrer des fichiers et courriels, afin de supprimer tout contenu exécutable, et n'autoriser que des formats maîtrisés.
- Nouveauté 2008: les 2 logiciels sont disponibles en logiciel libre...

Diode réseau

- Pour interconnecter 2 réseaux de niveaux de sécurité différents.
- Pour échanger des informations **dans un seul sens, du bas vers le haut**.
 - Exemple: recopier des pages web ou des courriels vers un réseau sensible.



Diode – partie matérielle



E : Emetteur  : Fibre optique connectée
R : Récepteur  : Fibre optique non connectée

- 2 transceivers (convertisseurs) RJ45 cuivre / fibre optique, 1 seule fibre est connectée.
- Peu coûteux, facile à mettre en place

BlindFTP: logiciel pour la diode

- But: transfert automatique de fichiers sur liaison unidirectionnelle **sans acquittement** (UDP)
- Implémentation prototype simple en Python
- Publié en 2007 sous **licence open-source CeCILL:**
- <http://decalage.info/python/blindftp>
- Contacts:
 - Philippe.Lagadec [à] nc3a.nato.int
 - Laurent.Villemin [à] dga.defense.gouv.fr

Diode – Applications

- **Transfert simple de fichiers / répertoires:**
 - L'utilisateur dépose un fichier dans son répertoire « dépôt » côté bas. (via FTP, partage Windows, ...)
 - Il le récupère sur le réseau sensible quelques secondes plus tard dans son répertoire « import ».
 - Avantages:
 - Plus souple et plus sûr qu'un support amovible
 - Garantie de l'unidirectionnalité
 - Possibilité d'appliquer une politique de filtrage
 - Possibilité de tracer les imports de fichiers
- **Mise à jour automatique de machines hors-ligne:**
 - Windows Update (WSUS), Linux, Antivirus, ...

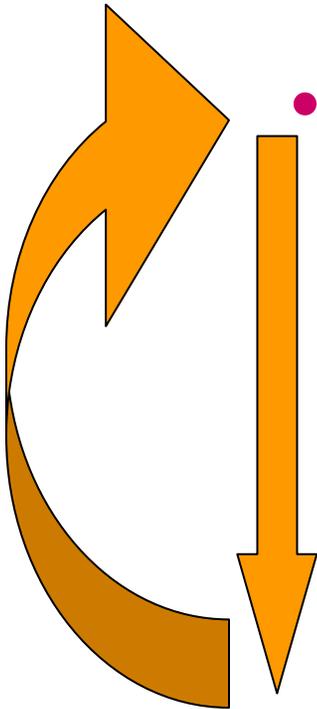
ExeFilter

- Framework générique pour filtrer des fichiers, courriels et contenus web
- Buts:
 - **1) S'assurer que seuls des formats maîtrisés sont autorisés (liste blanche)**
 - **2) S'assurer que tout contenu accepté est purement statique et inoffensif:**
 - suppression de tout contenu actif (macros, scripts, etc...)

projet ExeFilter

- Développé par DGA/CELAR depuis 2004, en Python.
- Publié en logiciel libre en 2008
 - licence CeCILL, compatible GPL
 - Suivi projet: DGA/CELAR et NATO/NC3A
- Extensible pour diverses applications:
 - Filtrage sur **passerelle**: Web, E-mail, Diode, ...
 - Filtrage sur **poste client**: clés USB, CD, DVD, ...
- Contacts:
 - Philippe.Lagadec [à] nc3a.nato.int
 - Arnaud.Kerreneur [à] dga.defense.gouv.fr

ExeFilter – principe



- **Chaque fichier est analysé:**
 - **Détection du format** suivant son **nom** et son **contenu**.
 - **Refusé** si format interdit par la politique.
 - Exécutables, scripts, formats inconnus, chiffrés, ...
 - **Nettoyé** s'il contient du code actif
 - Macros dans docs Office, scripts dans HTML, ...
 - **Accepté** tel quel si inoffensif
 - Texte simple, images bitmap, ...
 - **Analyse antivirus** (détection d'exploits connus)
 - **Analyse récursive** si conteneur (archives Zip, ...)

Formats supportés (v1.1.0)

Formats	Active content	Default Action
Text	-	Accept
JPEG,PNG,GIF,BMP	-	Accept
Audio: MP3, WAV	-	Accept
Video: AVI	-	Accept
HTML	Scripts, Objects	Clean
PDF	JavaScript, Embedded files	Clean
Word, Excel, PPT	Macros, OLE Objects	Clean
RTF	OLE Objects	Clean
Zip archive	Compressed files	Clean
Any format	unknown, malformed, encrypted	Block

Conclusion

- ExeFilter et BlindFTP: Deux projets (a priori) très intéressants, peu d'équivalents sur le marché
- Prototypes: Encore beaucoup d'idées à essayer, peu de temps pour coder. ;-)
- **Nous recherchons des contributeurs !**
 - Tests sur diverses plate-formes, sécurité/fuzzing, ajout de nouveaux formats, intégration avec divers proxies/relais/antivirus, documentation, ...
- Projets: <http://www.decalage.info/sstic06>