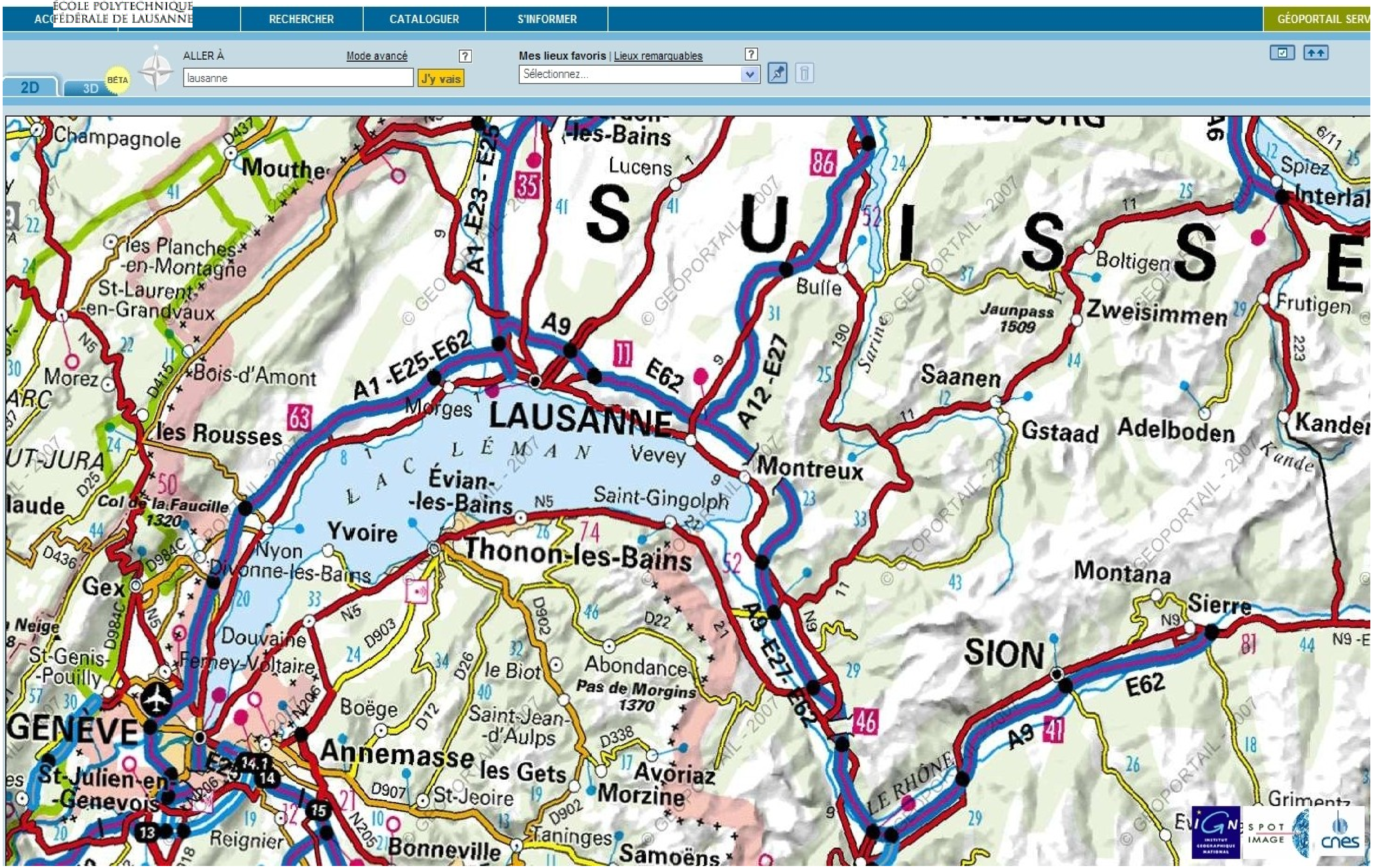
Quarantaine & Remédiation

- D'où parlons-nous ?
  - D'un campus qui ressemble à tous les autres
  - D'un pays qui ressemble assez à la France
- Qui sommes-nous ?
  - Des gens comme vous !
- De quoi parlerons-nous ?
  - D'une situation que vous connaissez bien !


RECHERCHER
CATALOGUER
S'INFORMER
GÉOPORTAIL SERV
ALLER À
Mode avancé
lausanne
J'y vais
Mes lieux favoris | Lieux remarquables
Sélectionnez...
2D
3D
BÊTA
SUISSE
LAUSANNE
LAC LÉMAN
GENÈVE
SION
Champagnole
Mouthe
Lucens
Bulle
Boltigen
Spiez
Interlal
Frutigen
Zweisimmen
Jaunpass 1509
Saanen
Gstaad
Adelboden
Kander
les Planches-en-Montagne
St-Laurent-en-Grandvaux
Morez
Bois-d'Amont
les Rousses
Col de la Faucille 1320
Gex
Morges
Vevey
Montreux
Évian-les-Bains
Saint-Gingolph
Yvoire
Thonon-les-Bains
Nyon
Divonne-les-Bains
Douvaine
Ferney-Voltaire
St-Genis-Pouilly
St-Julien-en-Genevois
Annemasse
Boëge
le Biot
Abondance
Pas de Morgins 1370
Saint-Jean-d'Aulps
les Gets
Avoriaz
Morzine
St-Jeoire
Taninges
Samoëns
Bonneville
Reignier
Montana
Sierre
Grimentz
LE RHÔNE
A1-E25-E62
A1-E23-E25
A9
E62
A12-E27
A9-E27-E62
© GEOPORTAIL - 2007
IGN
SPOT IMAGE
cnes

Motivation (1)

Juillet 2003

- Plus de 10000 ordinateurs raccordés à Internet
- Environ 6000 PC avec Windows
  - Souvent mal gérés donc vulnérables...
- Presque tous raccordés directement sur un port de nos équipements
  - Peu de micro-commutateurs
  - Début du déploiement WiFi...

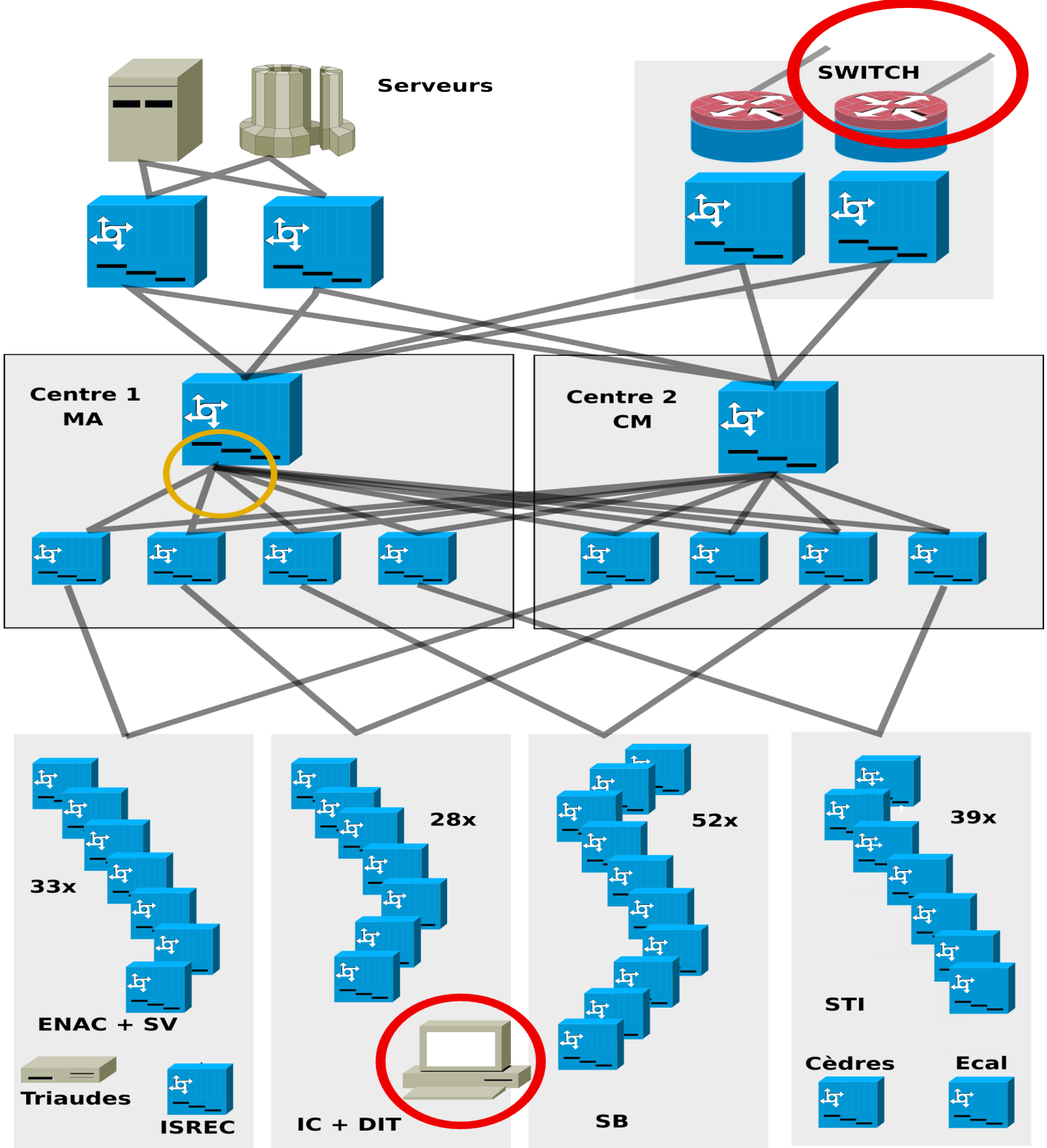
Motivation (2)

- Un grand nombre de PC victimes d'un ver ont une intense activité réseau
  - Scan 445/tcp faille LSASS

    135/tcp faille RPC/DCOM

Que faire ?

- Les couper totalement du réseau ?
- Les couper seulement d'Internet en les laissant polluer l'intranet ?


Serveurs
SWITCH
Centre 1
MA
Centre 2
CM
33x
ENAC + SV
Triaudes
ISREC
28x
IC + DIT
52x
SB
39x
STI
Cèdres
Ecal

Choix PP | Dans PP

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

BDPP

BDPP : MA_BC

Selectionner un autre Patch

Sortir

Equipement = CA-DIT-BC-1 Carte : 3/ 11 (dit-dyn VLAN 11)

Lib□rer

Annuler

les cables

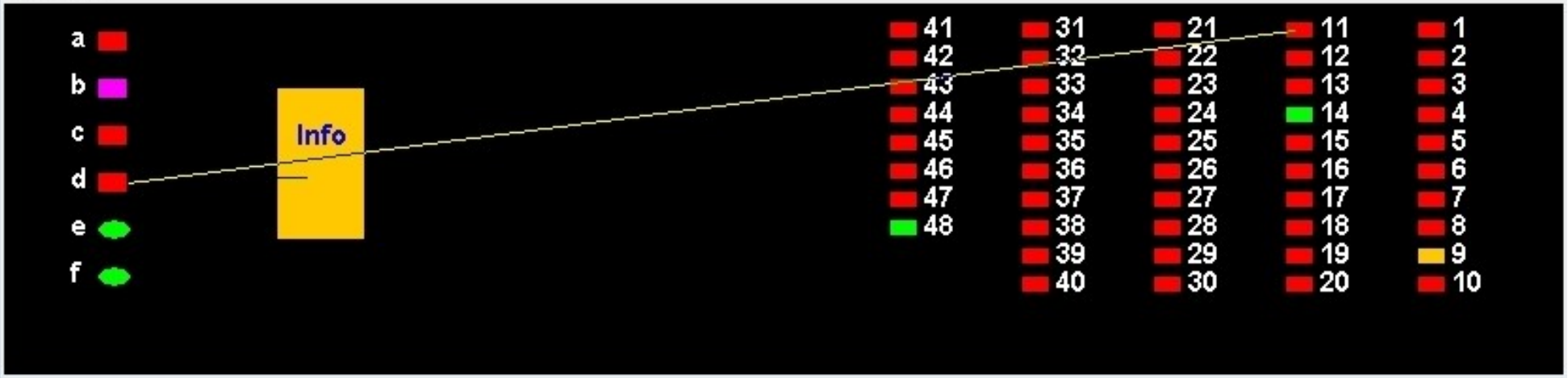
MA.B0.462
MA.B0.466
MA.B0.467

Equipements

Carte 3	128.178.111.65
1	BIDON-NORTEL
2	CA-DIT-BC-1
3	CA-MA-BC-1
4	CA-MA-BC-2
5	CY-MA-BC-2
6	SUNRAY-MA-BC
	sw-ma-bc-rescue

ca-dit-bc-1

Grapheur



Informations

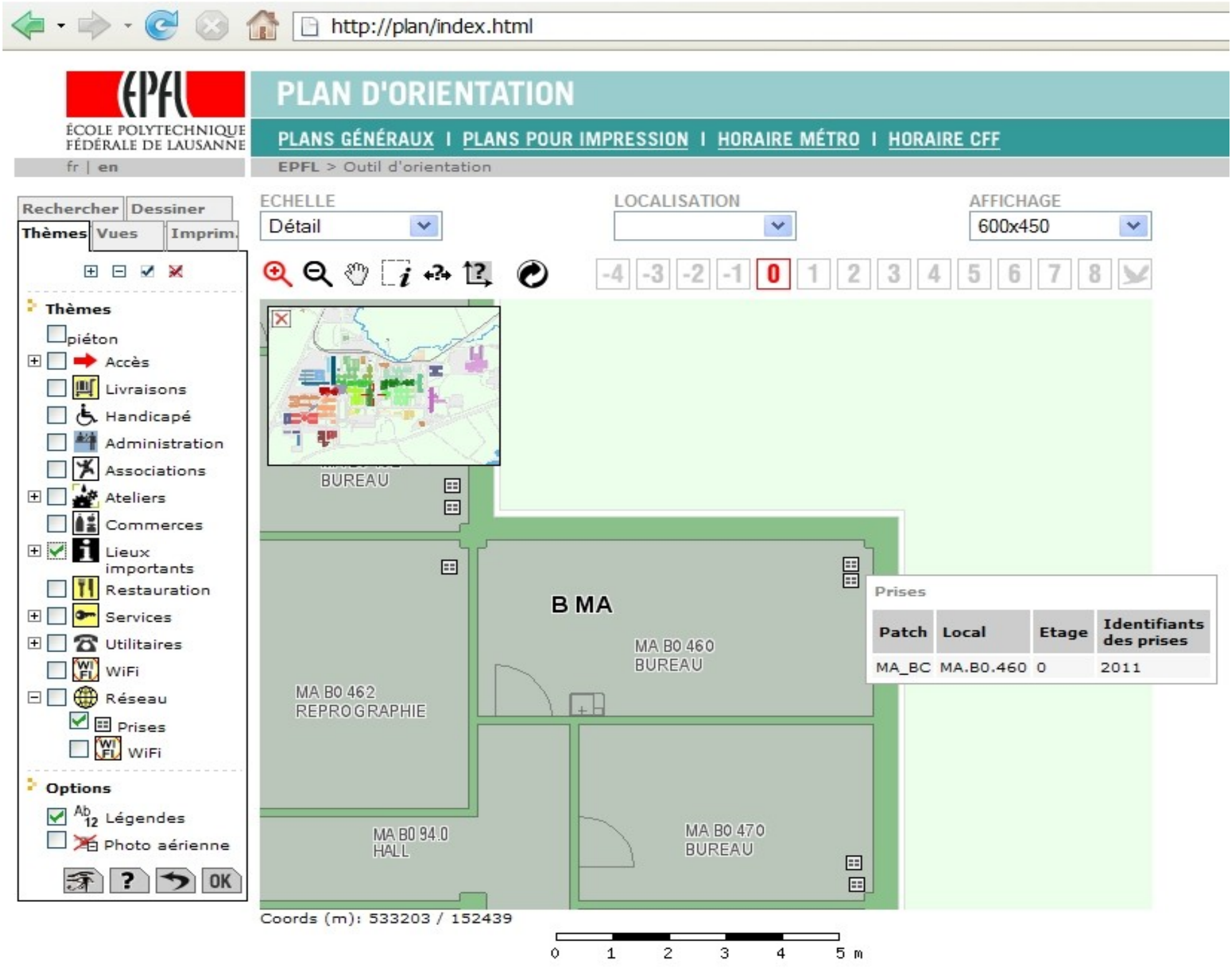
Carte de type Ether 10/100/1000 TX 48p RJ45...
Ma position est 5
Prises du cable 2011
Prises du cable 2012
Prises du cable 2011
On a trouve CA-DIT-BC-1 CARTE EN POSITION 3
Carte de type Ether 10/100/1000 TX 48p RJ45 AL...
Ma position est 3

Vlan

Gestion VLAN

Config PORTS

Etat des ports ou prises


http://plan/index.html
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
fr | en
PLAN D'ORIENTATION
PLANS GÉNÉRAUX | PLANS POUR IMPRESSION | HORAIRE MÉTRO | HORAIRE CFF
EPFL > Outil d'orientation
Rechercher
Dessiner
Thèmes
Vues
Imprim.
Thèmes
piéton
Accès
Livraisons
Handicapé
Administration
Associations
Ateliers
Commerces
Lieux importants
Restauration
Services
Utilitaires
WiFi
Réseau
Prises
WiFi
Options
Légendes
Photo aérienne
OK
ECHELLE
Détail
LOCALISATION
AFFICHAGE
600x450
-4 -3 -2 -1 0 1 2 3 4 5 6 7 8
BUREAU
B MA
MA B0 460
BUREAU
MA B0 462
REPROGRAPHIE
MA B0 94.0
HALL
MA B0 470
BUREAU
Prises
Patch
Local
Etage
Identifiants des prises
MA_BC
MA.B0.460
0
2011
Coords (m): 533203 / 152439
0 1 2 3 4 5 m

Quarantaine

- Confectionner un réseau spécial pour ces machines et les y glisser à la détection de l'activité malveillante
  - Mise en place d'un VLAN
  - L'équiper d'un automate pour rendre les services essentiels et assurer la communication avec l'intranet et l'Internet

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

QUARANTAINE QUARANTINE

Vous êtes dans un réseau en quarantaine!

You are in a quarantine network !

Votre ordinateur est atteint d'un **virus** ou d'un **vers** et génère un trafic très important et **dangereux** sur le réseau. Il nous a été nécessaire de l'isoler sur ce réseau de quarantaine.

Le but de ce réseau est quadruple :

- Vous **avertir** de ce qui vous arrive et vous donner les moyens de vous informer
- Vous **isoler** d'EPNET et d'Internet pour ne pas polluer d'autres systèmes
- Vous **donner accès** aux outils de nettoyage et aux patchs indispensables à appliquer
- Vous permettre de **revenir le plus vite possible sur EPNET**

Pour savoir quel virus infecte votre ordinateur et **comment le réparer**, il faut cliquer **ICI**.

Si vous n'arrivez pas à vous en sortir, demandez l'**aide** de l'équipe d'EPNET.

Your computer is infected by a **virus** or a **worm** and generate an huge and dangerous traffic on the network. So the network team has decided to isolate it into this quarantine network.

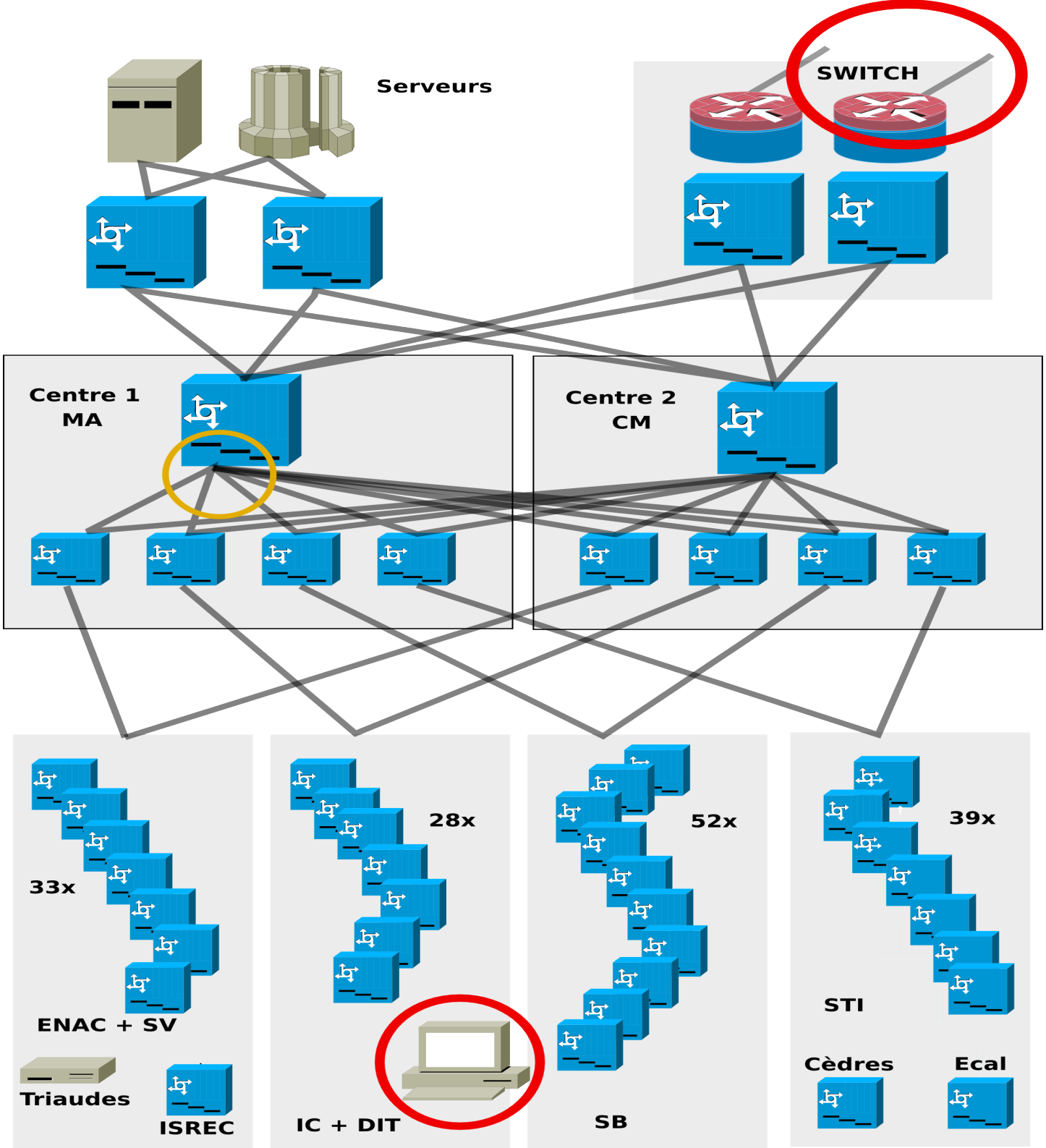
Click **HERE** to know what kind of virus you have and how to come back in the true network !

Services offerts

- DNS et DHCP
- Information précise par le web
  - Un proxy transparent est une solution facile à mettre en oeuvre et efficace
- Communication entre l'agent antivirus du poste et son serveur EPFL
- Permettre des mises à jour du système
- Permettre à l'utilisateur d'en sortir en s'authentifiant

Quarantaine Détection (1)

- Une sonde Snort bien placée sur le réseau permet de détecter (encore) les scans que font les vers et bots...
- Rendant possible le changement du Vlan du port sur lequel la machine infectée est connectée
  - Automatiquement
  - Rapidement
  - N'importe quand


Serveurs
SWITCH
Centre 1
MA
Centre 2
CM
33x
ENAC + SV
Triaudes
ISREC
28x
IC + DIT
52x
SB
39x
STI
Cèdres
Ecal

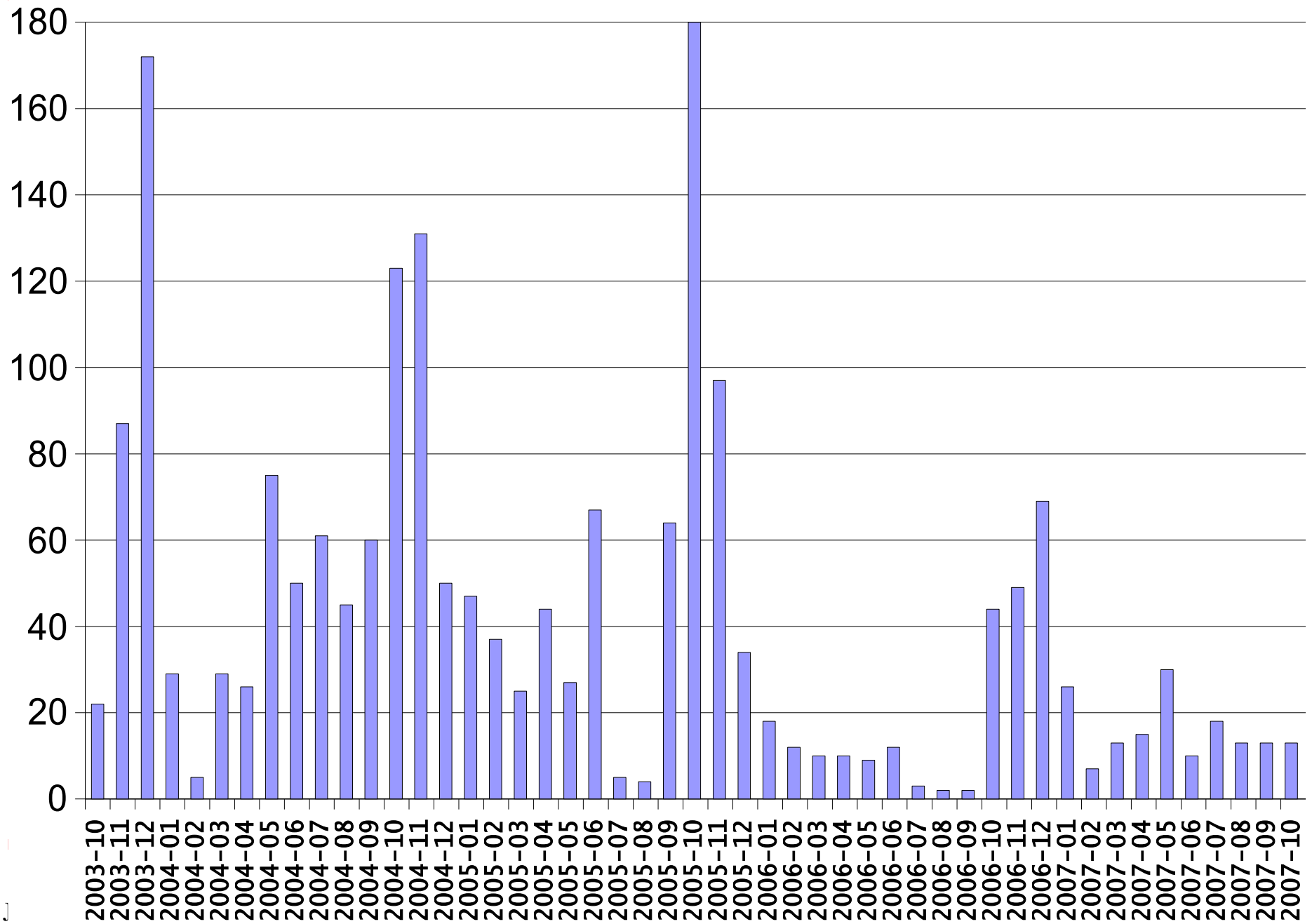
Quarantaine Détection (2)

- Les botnets sont de plus en plus furtifs, il faudra adapter les méthodes de détection à leurs comportements.

- Notre fournisseur d'accès au réseau académique (SWITCH) nous prévient aussi de l'appartenance de nos machines à des botnets.
  - Alors la mise en quarantaine est manuelle

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Machines en quarantaine



Bilan

- Les utilisateurs des machines qui sont passées par la quarantaine n'ont pas été désarçonnés
  - La situation leur est apparue claire
  - La plupart s'en sont sortis seuls et vite
- Pour l'équipe sécurité comme pour nous au réseau, la situation aussi est claire
- De moins en moins de PC sous Windows tombent en quarantaine, on a l'impression d'avoir assaini notre parc...

Perspectives

- Nous adapter à l'évolution des agents malveillants
  - Continuer à travailler sur des détecteurs
    - Maintenir notre IDS
    - Chercher d'autres moyens
- Nous adapter à l'évolution du réseau
  - Wifi
  - Nomadisme
    - Mettre en quarantaine derrière les concentrateurs VPN

Quarantaine & Remédiation

- Le nombre de machines appartenant à des botnets est alarmant
- *The Network is the infection* (Sous titre de l'article Botnet Detection and Response de David Dagon)
  - La mise en quarantaine permet d'agir
  - La remédiation de prévenir !

Remédiation Motivation

Permettre d'offrir des services semblables à ceux du réseau de quarantaine

à la demande

Telle est la raison d'être de ce réseau.

Reseau libre service

- Portail Captif

EPFL PUBLIC NETWORK **Help Desk : +41 21 693 1234**

Visitors — Click on the **EnClair** logo to **login** and access to **Internet** (or for help)

EPFL members — Students and staff use **WPA access** or start your **VPN client**
*Click on **SafeNetwork** logo to update safely your computer*

SWITCHmobile partners — Start your VPN client to access your **campus network**

Commercial Internet Access — Click on provider's icon

Ethernet
1000 prises

public-epfl

Accès à la Remédiation

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

SAFE NETWORK

Bienvenue dans le réseau de remédiation

SafeNetwork est un réseau de remédiation. On peut comparer SafeNetwork à la mise en **quarantaine volontaire** d'une machine. Depuis l'environnement réseau obtenu de SafeNetwork vous pouvez atteindre les outils nécessaires à l'installation, la réparation et l'audit du système d'exploitation de votre ordinateur.
Dans le mode SafeNetwork, votre machine est moins exposée aux attaques en provenance de machines malveillantes.

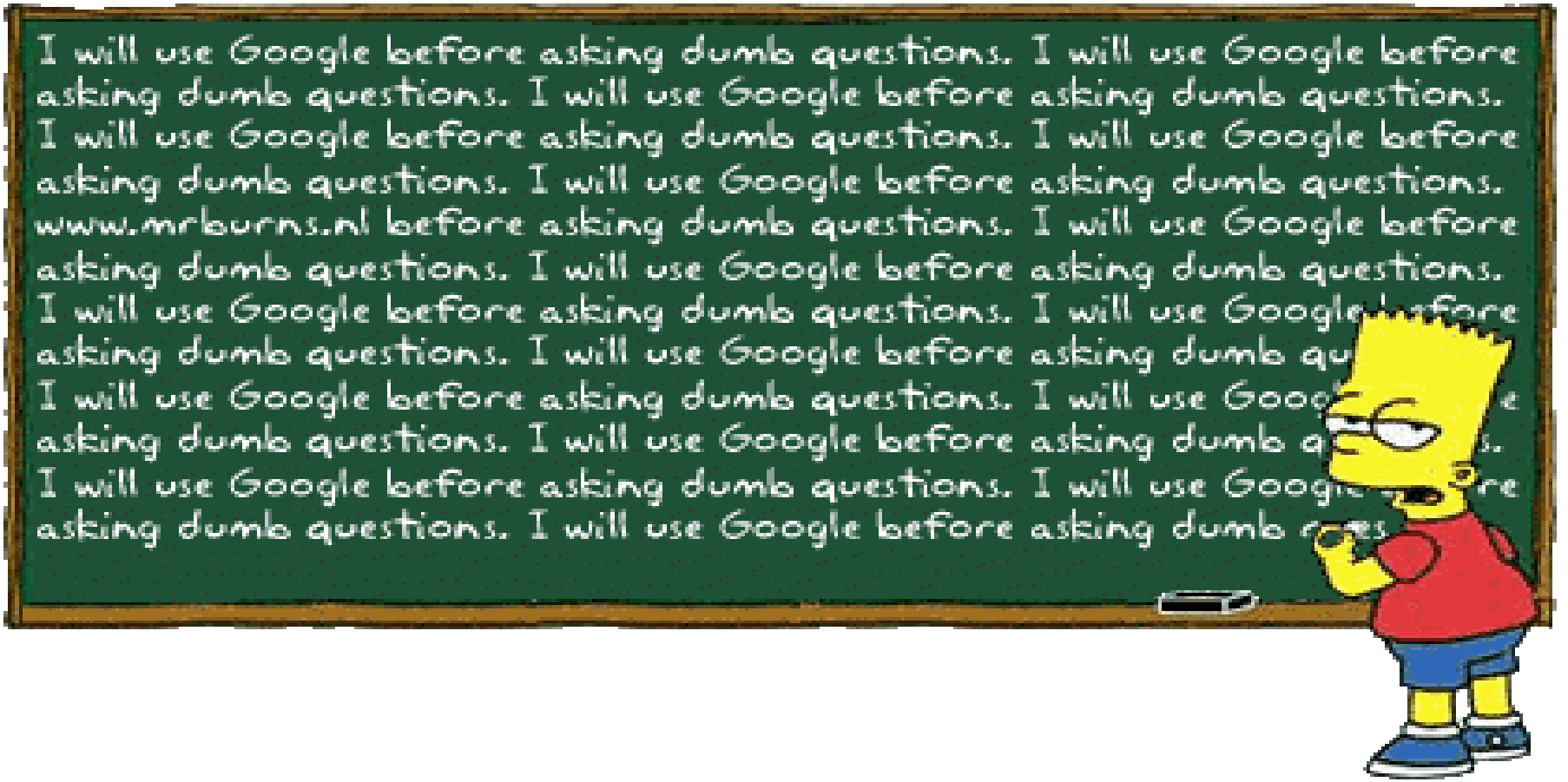
Welcome inside SafeNetwork

We can describe the Safe Network as an **opt-in quarantine**. From the Safe Network environment you have access to the tools needed for patching, updating and auditing your computer's operating system.
Inside the Safe Network, your computer is less prone to be remotely infected by outside rogue systems.

available **SERVICES** disponibles:

- Réaliser une mise à jour par Windows update
- Accéder aux outils et aux informations de Microsoft

Questions et...



réponses...