

Communiqué du secrétariat général de dot-root

info@dot-root.com

***Parce que l'Internet
est attaqué***

**la France et l'Europe n'en doivent
pas pour autant être 'e-colonisées'**

Le système central de l'Internet a été très gravement attaqué lundi. Pour le comprendre, et comprendre les implications pour la France et l'Europe, commentons CNN.

Internet est une immense ville virtuelle avec ses rues physiques (les lignes), leurs numéros (adresses IP) et l'annuaire des noms (de domaine) des résidents (DNS). Ce DNS permet de dire à quelle adresse numérique se trouve un site dont on connaît le nom, et donc aux commutateurs (transport urbain) par quelle rue passer.

Le contrôle de l'Internet, et donc de l'accès aux ressources mondiales en ligne, est assuré par ce DNS. Son cœur est la table des suffixes (".com", ".fr"). Pour trouver l'adresse IP de <http://elysee.fr>; on demande d'abord au système central (système racine) où est l'ordinateur qui connaît l'annuaire "fr". Puis on demande à cet ordinateur où est l'ordinateur qui héberge le site de l'Elysée. C'est très simple et très robuste. Sauf sur un point : la table des matières de 13 ordinateurs est unique. Elle est gérée par l'ICANN, dans le faits une antenne spécialisée partie du dispositif de la Maison Blanche en cours de finalisation, pour la défense du sol américain (Homeland) virtuel. Par son unicité, elle rend le monde vulnérable, attirant et rendant efficaces les attaques comme celle de lundi décrite ici, qui s'intensifie.

Le Conseiller de la Maison Blanche a publié un projet de plan d'effort de défense en cours de finalisation ces jours-ci (en particulier à la réunion de Shanghai de cette semaine) pour répondre mondialement à cette menace mondiale. Ce plan conduit à une "e-colonisation" américaine de la planète par la reconstruction d'un Internet sécurisé et donc nécessairement nord-américain en raison de la continuation naturelle des technologies, et la centralisation de des contrôles.

Le projet d'origine franco-européenne "<http://dot-root.com>" ouvert à tous – comme l'Internet - répond à cette perte de souveraineté de l'ensemble des Etats, en expérimentant une autre organisation du DNS où de nombreux systèmes racines sont gérés en parallèle total et ce qui annule l'intérêt et la portée d'une attaque, et permet un fort développement durable par la possibilité d'Internet de proximité comme le projet Webs de France (1000 Internet locaux en pré-opérations et 7000 à court terme).

Seven of the 13 servers failed to respond to legitimate network traffic and two others failed intermittently during the attack, officials confirmed.

The FBI's National Infrastructure Protection Center was "aware of the denial of service attack and is addressing this matter," spokesman Steven Berry said.

Service was restored after experts enacted defensive measures and the attack suddenly stopped.

The 13 computers are spread geographically across the globe as precaution against physical disasters and operated by U.S. government agencies, universities, corporations and private organizations.

La répartition est de 1 machine au Japon, 1 en Hollande et 1 en Suède, **4** sur la Côte ouest des **Etats-Unis**, **6** sur la côte est des **Etats-Unis**. 1 était au WTC le 11/9/2001.

"As best we can tell, no user noticed and the attack was dealt with and life goes on," said Louis Touton, vice president for the Internet Corporation for Assigned Names and Numbers, the Internet's key governing body.

M. Louis Touton est le Conseil Juridique de l'ICANN. L'ICANN a pour rôle réel de stabiliser sous son contrôle les partenaires du réseau par un maillage contractuel. Elle représente les opérations techniques assurées bénévolement par 13 entreprises, institutions et universités privées. Le projet **dot-root** vise à tisser et à tester une approche similaire (qui a fait ses preuves), mais faite de centaines de partenaires en concertation entre eux et avec leurs sociétés civiles, leurs Etats et leurs économies,.

"We were prepared, we responded quickly," said Brian O'Shaughnessy, a spokesman for VeriSign Inc., which operates two of the 13 computers in northern Virginia.

Verisign gère le système maître du système central (racine) du DNS, pour le compte de l'agence des télécommunications des Etats-Unis (NTIA), conseillée par l'ICANN.

Computer experts who manage some of the affected computers, speaking on condition of anonymity, said they were cooperating with the White House through its Office of Homeland Security and the President's Critical Infrastructure Protection Board.

Richard Clarke, President Bush's top cyber-security adviser and head of the protection board, has warned for months that an attack against the Internet's 13 so-called root server computers could be greatly disruptive.

Richard Clarke est l'auteur (<http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>) du projet d'effort de défense du Homeland virtuel. Il explique depuis le 11 septembre le danger pour les Etats-Unis et le besoin de défense de ce système. Jean-François Morfin, initiateur de dot-root explique aussi pour le monde – préconisant un e-OTAN – et expliquant que ce système doit être construit, non pas comme un château fort du moyen-âge sur-défendu et unissant l'industrie informatique sous bannière fédérale en un projet Manhattan II, mais en un système à la Vauban, chaque partie (pays) y étant autonome, en défense mutuelle concertée, motivée par sa souveraineté respectée, adaptée à ses intérêts locaux et, par là, moins attrayante et plus complexe à attaquer.

Il faut cependant savoir que le code des télécommunications américain (47 USC 230 (f)(1)) définit un Internet sans frontière et donc une **juridiction mondiale** du Congrès, que l'ICANN a pour mission d'établir par accords et que reprend le plan de Richard Clarke. Cette vision légale ne peut se traduire dans les faits, en raison de la nature même de l'architecture Internet à reconstruire du DNS à Windows (disparition des fichiers dans une base sécurisée) que par le besoin d'un contrôle sécuritaire mondial, donc technique (par là économique) et sur les données des personnes.

These experts said the attack, which started about 4:45 p.m. EDT Monday, transmitted data to each targeted root server 30 to 40 times normal amounts. One said that just one additional failure would have disrupted e-mails and Web browsing across parts of the Internet.

Le rapport de Richard Clarke montre que la conjonction de ce type d'attaques avec d'autres actions comme Code-Rouge (Virus) et des pénétrations, survenant de plus en plus, dans les systèmes d'infrastructures nationales (transport aérien, défenses, sécurité civile) ou pouvant provoquer la panique (média, banques, système de santé) place les Etats-Unis dans une situation de risque "équivalent nucléaire". Nous devons faire la même étude, bien que nous ne sommes pas "tout Internet".

Monday's attack wasn't more disruptive because many Internet providers and large corporations and organizations routinely store, or "cache," popular Web directory information for better performance.

"The Internet was designed to be able to take outages, but when you take the root servers out, you don't know how long you can work without them," said Alan Paller, director of research at the SANS Institute, a security organization based in Bethesda, Maryland.

C'est le rôle premier de **dot-root**. Disposer dès aujourd'hui d'un système de secours en opérations de test mais capable de prendre un relais immédiat, en ayant au moins l'un de ses systèmes dupliquant celui de l'ICANN, et les autres systèmes (à terme des centaines de machines) capables de venir en renfort. **dot-root**, qui vise à être en opérations réelles pour la fin de l'année, veut passer des accords de procédures avec les Etats pour établir les conditions pratique de son aide de crise et pour développer des solutions de priorité de services, civiles ou militaires.

Although the Internet theoretically can operate with only a single root server, its performance would slow if more than four root servers failed for any appreciable length of time. In August 2000, four of the 13 root servers failed for a brief period because of a technical glitch.

dot-root vise plusieurs centaines de serveurs, techniquement indépendants de A à Z.

Pour toute information sur l'ICANN <http://www.icann.org>

sur la position de la Maison Blanche <http://www.whitehouse.gov/pcipb/>
President's Critical Infrastructure
Protection Board

sur dot-root <http://dot-root.com>
études en souscription ou gratuites <http://utel.net/u-docs.shtml>

Le projet dot-root a été engagé, début septembre 2002, après deux ans de préparation, par un consortium de serveurs racine, dont les trois premiers systèmes sont administrés par

UTEL	France	:	Jean-François C. (Jefsey) Morfin
Boroon	Allemagne	:	Pascal Bernhard (Président de dot-root)
ORSN	Allemagne	:	Markus Grundman

formant son comité d'administration.

La promotion du projet est assurée par un Steering Committee en cours de constitution et son conseil technique par in Advisory Committee ouvert à tout professionnel du DNS. Son Relational Committee lui permet de tisser et déjà de maintenir des relations parfois poussées avec les organisations internationales, gouvernementales ou para-gouvernementales, des ONG, des entreprises

Dot-Root a été créé conformément à la doctrine de l'ICANN (document ICP-3) quant à la gestion et à l'expérimentation communautaire du DNS et de l'administration des noms de domaines. Il s'agit d'un projet Internet donc d'initiative bénévole, et ouvert à tous, monté grâce à des aides financières et matérielles et la proposition d'études.

dot-root est en cours de mise en place depuis début septembre 2002 après une période de développement et de validation technique engagée en octobre 2000.