LES PEURS DES CYBERDÉFENSEURS

LE 29 OCTOBRE 2012 ***PIERRE ALONSO***

Les responsables français de la cyberdéfense ont parfois des sueurs froides. Le contre-amiral Coustillière et le directeur de l'Agence nationale de la sécurité des systèmes d'informations ont décrit quelques scénarios catastrophes la semaine dernière.

Un "Pearl harbor numérique" ? À intervalles réguliers, l'expression revient dans le bouche de responsables de la cyberdéfense, surtout américains. Le sécretaire de la Défense, Léon Panetta, **a exprimé** ses craintes d'une telle cybercatastrophe lors d'un discours à New York le 11 octobre dernier.

En France, l'expression n'est pas employée en l'état, mais les craintes existent. Elles ont été exprimées publiquement la semaine dernière par les deux principaux responsables de la cyberdéfense. Le contre-amiral Coustillière a été nommé officier général à la cyberdéfense le 1er juillet 2011. Il est entre autres à la tête du centre d'analyse en lutte informatique défensive, le Calid.

"Un espace de confrontation"

Dans son intervention **organisée par le cercle Défense et Stratégie** mercredi, il a décrit son cauchemar. Un plan simple, en plusieurs temps, qui pourrait aboutir à des dommages irréversibles. Et de rappeler qu'un *"changement de dimension"* s'est produit depuis quelques années, faisant du cyberespace *"un espace de confrontation, quelque soit le nom qu'on lui donne"*. Une précaution oratoire pour éviter le terme contesté de cyberguerre…

Le contre-amiral Coustillière a évoqué un plan en trois temps, trois phases distinctes qui ne peuvent être menées que par *"une structure"* importante, avec un niveau élevé de renseignement. Comprendre, plutôt par un État que par un petit groupe de pirates informatiques.

La première phase vise à désorganiser la cible (là encore un État) : fausses rumeurs et mouvements de protestations sur les réseaux sociaux, attaques par dénis de service (DDoS) sur les sites institutionnels (les sites de députés par exemple), puis attaques de réseaux locaux peu protégés. La seconde phase vise à *"désorganiser la société"* . Les services de sécurités sont monopolisés, leurs moyens saturés.

En cause : des attaques sur installations vitales, en cherchant *"le maillon faible"* sur ces systèmes déjà bien protégés, ainsi que de nouvelles attaques par dénis de service ciblant des banques. Le climat est alors propice pour lancer des actions offensives plus complexes, avec des répercussions potentiellement mortelles. Sur les infrastructures de transport par exemple.

L'âge du cyberespionnage

Ainsi dépeint, le tableau ressemble à une **dystopie** cyberpunk. Un scénario catastrophe plus lointain que l'espionnage via Internet, grande préoccupation du moment :

> ***Des gigas [octets] de données s'échappent de nos industries.***

Préoccupation largement partagée par Patrick Pailloux, le directeur de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), second bras armé de la cyberdéfense. Quatre sujets l'empêchent, plus ou moins, de dormir, **a-t-il expliqué** à l'institut des hautes études de la défense nationale : la cybercriminalité, les tentatives de déstabilisation, le sabotage et le cyberespionnage donc.

"À côté de ce qui se passe aujourd'hui, c'était de la gnognote la guerre froide" attaque-t-il. Un *modus operandi* basique par exemple, disponible au patron un peu dégourdi qui traîne *"sur des forums underground"* , parle anglais et dispose de quelques centaines d'euros. Usurper l'identité d'un proche de la cible (au hasard, un concurrent), envoyer un email depuis cette fausse identité à la cible.

BERCY, LE PIRATAGE QUI TOMBE À PIC

Faut-il avoir peur du piratage de 150 ordinateurs au ministère de l'Economie et des Finances? C'est surtout l'occasion pour ...

Au mail est attaché une pièce jointe, un cheval de Troie, acheté sur Internet. *"Des usines à fabriquer des virus"* permettent de changer les signatures chiffrées des logiciels malveillants. En somme, d'empêcher les antivirus de les identifier et donc de les rendre inopérants. Un peu de débrouillardise, quelques poignées d'euros et un zeste de renseignements suffisent pour obtenir des informations confidentielles sur ses concurrents. Des pratiques interdites, mais courantes.

Conclusions communes des deux hauts responsables : améliorer l'hygiène informatique et préparer la résilience des citoyens. A cette fin, une réserve citoyenne pour la cyberdéfense **est en cours de création** et les cyberdéfenseurs se chargent de faire passer le message.

Photo par **Teymur Madjderey** [CC-byncnd]

JO SOP
le 29 octobre 2012 - 19:12 • SIGNALER UN ABUS - PERMALINK

Le Ministère de la Défense français est actuellement incapable de régler un problème de logiciel de paiement des soldes de ses piou-pioux dont certains sont contraint d'emprunter aux banques pour faire vivre leur famille.
Alors la cyber-défense ? Laissez-moi rire !

VOUS AIMEZ 7 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CORRECTOR
le 2 novembre 2012 - 20:58 • SIGNALER UN ABUS - PERMALINK

> attaques par dénis de service (DDoS) sur les sites institutionnels (les sites de députés par exemple),

Ah oui, si le site de Nadine Morano est indisponible pendant 24 heures, la République est en danger…

C'est un gag?

> les signatures chiffrées des logiciels malveillants.

Pardon?

signature chiffrée = charabia

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PIERRE ALONSO
le 3 novembre 2012 - 15:57 • SIGNALER UN ABUS - PERMALINK

Bonjour Corrector,

Vous avez bien noté que les DDoS sur des sites institutionnels intervenaient dans la première phase et qu'ils n'avaient pas pour objet de mettre directement la République en danger (ce n'est pas un gag) ?

Quant à la signature chiffrée des malwares, évoquée par Patrick Pailloux, merci pour votre remarque synthétique, n'hésitez pas à développer, Corrector, si le cœur vous en dit.

Cordialement,

PA

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CORRECTOR
le 3 novembre 2012 - 16:29 • SIGNALER UN ABUS - PERMALINK

> Bonjour Corrector,

Bonjour Pierre,

> Vous avez bien noté que les DDoS sur des sites institutionnels intervenaient dans la première phase et qu'ils n'avaient pas pour objet de mettre directement la République en danger (ce n'est pas un gag) ?

La première phase d'une attaque n'est pas destinée à provoquer directement la défaite de l'ennemi, mais de la préparer, et d'y contribuer indirectement. Je ne vois pas en quoi les attaques contre des sites vitrines permet de contribuer d'une façon quelconque à quoi que ce soit à part le cirque médiatique habituel : le site Web de la Maison blanche, et la CIA … a été piraté : hou hou hou qu'est-ce qu'on a peur!

> Quant à la signature chiffrée des malwares, évoquée par Patrick Pailloux, merci pour votre remarque synthétique, n'hésitez pas à développer, Corrector, si le cœur vous en dit.

Je veux juste dire que "signature chiffrée des malwares" ne veut rien dire du tout. Qu'est-ce que le terme "chiffré" vient faire ici? On parle de cryptographie, ou bien quoi?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Les peurs des cyberdéfenseurs « Cybercriminalité, cyberdéfense, cyberguerre,cybersécurité, cyberterrorisme, … le 31 octobre 2012 - 11:08

[...] En savoir plus Évaluez ceci :Share this:ShareLinkedInTwitterJ'aime ceci:J'aimeSoyez le premier à aimer ceci. [...]