RFC 8073 : Coordinating Attack Response at Internet Scale (CARIS) Workshop Report

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mars 2017

Date de publication du RFC : Mars 2017

https://www.bortzmeyer.org/8073.html

Ce nouveau RFC fait le bilan de l'atelier CARIS <https://www.iab.org/activities/workshops/caris/> ("*Coordinating Attack Response at Internet Scale*") qui s'est tenu à Berlin le 18 juin 2015. Cet atelier avait pour but d'explorer les problèmes de coordination entre les victimes et témoins d'une attaque portant sur l'Internet. Ce RFC est un compte-rendu, les positions exprimées ne sont pas forcément celles de l'IAB ou de l'Internet Society (organisateurs de l'atelier). D'autant plus que les participants ont mis les pieds dans le plat, expliquant très bien pourquoi il n'y a toujours pas de coordination globale des acteurs de l'Internet face aux attaques. (Un deuxième atelier sur ce thème a eu lieu en 2019, et son compte-rendu figure dans le RFC 8953 [1].)

L'atelier <https://www.iab.org/activities/workshops/caris/> avait été organisé pour que les participants à la réunion FIRST de Berlin puissent venir. Il rassemblait cinquante acteurs (c'était un atelier fermé, sur invitation seulement) de l'Internet, représentant une grande diversité d'organisations. La liste des participants figure dans l'annexe A du RFC. Chaque participant avait rempli un article de deux pages expliquant son point de vue et/ou les problèmes qu'il·elle souhaitait aborder. Tous ces documents sont disponibles en ligne <https://www.iab.org/activities/workshops/caris/agenda/> (je vous encourage à les lire). Dans le reste du RFC, n'attendez pas d'attribution de tel discours à tel participant, l'atelier était tenu sous la règle de Chatham House, pour que les discussions restent libre.

L'atelier a vu cinq sessions (cf. section 2 du RFC) autour de ce thème des attaques, et de la coordination pour y faire face :

— Coordination entre les CSIRT, et avec ceux qui combattent directement l'attaque,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8953.txt

— Répondre aux dDoS et aux botnets, avec passage à l'échelle pour les attaques de grande ampleur que nous voyons aujourd'hui,
— Infrastructure de l'Internet, notamment les acteurs du DNS, et les RIR,
— Problèmes de confiance et de confidentialité dans les échanges entre acteurs de l'Internet (un très gros sujet lors de l'atelier),
— Conséquences des attaques sur l'architecture de l'Internet, et sur ses futures évolutions. (Peu de détails données dans le RFC sur cette dernière session.)

Parmi les organisations qui ont participé à la première session, on notait, entre autres :

— L'ENISA qui, quoiqu'elle fasse de la formation et de l'échange, n'a pas directement d'activité concernant les attaques pendant qu'elles se produisent (l'ENISA n'est pas « temps réel »).
— L'APWG, qui a un mécanisme d'échange entre acteurs (une "*clearing house*").
— Le Ren-ISAC <http://www.ren-isac.net/> (si vous ne savez pas ce qu'est un ISAC, c'est le moment d'apprendre) qui sert de point de partage d'informations dans le monde académique états-unien. Cet organisme permet une mutualisation des efforts (bien des universités n'ont pas les moyens d'avoir une équipe à temps plein pour réagir aux attaques 24 heures sur 24).
— Le CERT brésilien, qui joue un rôle essentiel dans ce pays. Bien des pays, contrairement au Brésil, n'ont pas un CERT national mais plein de petits CERT limités à un groupe ou une entreprise.

Les principaux points mis en avant pendant cette session ont été :

— La surveillance de masse effectuée par les États a mis en danger les mécanismes de coordination, en réduisant la confiance. On note qu'au contraire de tant de colloques bavards et convenus sur la cybersécurité, l'atelier CARIS n'a pas pratiqué la langue de bois. Au lieu de répéter en boucle que la cybersécurité était importante, qu'elle reposait sur l'échange et la coordination, les participants ont directement pointé les vrais problèmes : les acteurs n'ont pas confiance dans l'État, et pour des très bonnes raisons, ce qui diminue l'éfficacité du travail en commun.
— Les tentatives des certains États d'encourager le partage d'informations (par exemple via une agence nationale) n'ont pas été des succès.
— Tout le monde veut que **les autres** partagent de l'information mais personne ne veut en donner. Ici encore, l'atelier pointe un problème que tout le monde connait, mais dont on ne parlait pas publiquement.
— Outre les simples problèmes d'ego, le partage d'informations est handicapé par les craintes des organisations pour leur réputation : si on dit la vérité sur une attaque qu'on n'a pas bien paré, on va paraitre faible.
— Les barrières de langue sont un gros problème. (Le RFC ne le dit pas, mais tout le monde pense aux immenses difficultés de communication avec les acteurs chinois. Des listes de diffusion comme celles de NANOG sont pleines de remarques amères « j'ai signalé le problème au FAI chinois et il n'a rien fait », sans que leur auteur se demande comment **lui** réagirait s'il recevait un rapport d'attaque écrit en mandarin. Contrairement à ce que pourrait laisser croire un certain discours globaliste, tout le monde ne parle pas anglais. Sans compter les problèmes culturels, encore plus difficiles.)
— Les règles de protection de la vie privée (comme le réglement européen sur la protection des données personnelles) peuvent gêner l'échange d'information (on n'envoie pas un fichier contenant des adresses IP aux USA). (Derrière cette remarque, on peut lire l'agacement des États-Unis - qui eux-même n'envoient pas de données - face aux lois européennes plus protectrices, mais aussi le regret des professionnels de la lutte contre les attaques informatiques, face à des lois prévues pour traiter d'autres problèmes que les leurs.)

Deuxième session, sur les mesures de lutte contre les dDoS et les botnets, notamment sur la question du passage à l'échelle de ces efforts. Les points essentiels abordé furent :

— Les mesures prises jusqu'à présent ont été plutôt efficaces. (C'était avant l'attaque contre Dyn, et le RFC ne mentionne pas le fait que la plupart de ces « mesures efficaces » ne sont accessibles qu'aux gros acteurs, ou à leurs clients, et que le petit hébergeur reste aussi vulnérable qu'avant.)
— La tension entre les réactions à court terme (stopper l'attaque en cours) et les exigences du long terme (éradiquer réellement le botnet, ce qui implique de le laisser « travailler » un certain temps pour l'étudier) reste entière. Sans compter, là aussi, le manque d'échanges entre pompiers de la lutte anti-dDoS et chasseurs de botnets.

— Il existe des groupes où règne une certaine confiance mutuelle comme le peu documenté CRAG <https://www.iab.org/wp-content/IAB-uploads/2015/04/CARIS_2015_submission_21.pdf>.
— Trier le trafic entrant, puis le filtrer, est un problème soluble. (Je note personnellement que, pour l'instant, les seules solutions sont des boîtes noires fermées. Un problème pour les gens attachés à la liberté.)
— Il existe un groupe de travail IETF nommé DOTS <https://tools.ietf.org/wg/dots> qui travaille sur des mécanismes techniques facilitant l'échange de données pendant une attaque. Un effort précédant de l'IETF avait mené au RFC 6545. Les deux solutions sont conceptuellement proches mais DOTS est plus récent, devrait utiliser des techniques modernes et semble avoir davantage de soutiens de la part des acteurs.
— Il existe une certaine dose de confiance dans le milieu mais pas complète. On ne peut pas toujours faire confiance aux informations reçues. À cette session également, le problème des services d'espionnage étatiques a été mentionné, comme une grosse menace contre la confiance.
— La question brûlante des « arrêts automatiques » ("*automated takedowns*") a été mentionnée. Certains cow-boys voudraient, compte-tenu de la rapidité des phénomènes en jeu, que certaines décisions puissent être automatiques, sans intervention humaine. Par exemple, un nom de domaine est utilisé pour une attaque « "*random QNAMEs*" <https://indico.dns-oarc.net/event/20/session/3/contribution/37> », l'attaque est analysée automatiquement, signalée au registre et paf, le nom de domaine est supprimé. Inutile de dire que l'idée est très controversée.

Ensuite, troisième session, consacrée aux organisations de l'infrastructure DNS (par exemple les registres) et aux RIR. Les points étudiés :

— L'utilisation du "*passive DNS*" (par exemple DNSDB <https://www.bortzmeyer.org/dnsdb.html>) pour analyser certaines attaques.
— Les données que détiennent les RIR, en raison de leur activité mais aussi suite à divers projets non directement liés à leur activité (comme l'observation des annonces BGP ou comme la gestion d'un serveur racine du DNS). Des participants ont regretté l'absence d'API standard pour accéder à ces données.
— Certains des RIR ont déjà une coordination active avec des organisations qui réagissent en cas d'attaques.

Quatrième session, les problèmes de confiance. Tout le monde est d'accord pour dire que c'est cool de partager les données, et que c'est indispensable pour lutter efficacement contre les attaques. Alors, pourquoi si peu d'organisations le font ? Il n'y a clairement pas une raison unique. C'est un mélange de crainte pour la vie privée, de contraintes juridiques, de problèmes techniques, de différences culturelles et de simples malentendus. Sans compter le pur égoïsme (« partager **mes** données avec nos concurrents ??? ») Enfin, il faut rappeler qu'il est impossible de s'assurer du devenir de données numériques : si on passe nos données à quelqu'un, pour aider pendant une attaque, que deviendront-elles après ? (Envoyer des données aux USA, c'est la certitude qu'elles seront vendues et revendues.) Le RFC note que tous les participants à l'atelier ont estimé que ces raisons étaient mauvaises ou, plus exactement, qu'on pouvait trouver des solutions. Les points précis discutés :

— La réputation est cruciale : il y a des gens à qui on envoie toutes les données qu'ils veulent et d'autres à qui on ne transmettra rien. (Sans la règle de Chatham House, on peut parier que personne n'aurait osé exprimer cette évidence pendant l'atelier.)
— L'utilisation du TLP (certains participants regrettent son manque de granularité, je pense personnellement que déjà trop de gens ont du mal avec ses quatre niveaux).
— Officielement, la confiance est entre organisations. En réalité, elle est entre individus (personne ne fait confiance à un machin "*corporate*") et il faut donc développer des liens entre individus. En outre, la confiance est forcément limitée en taille : on ne fait confiance qu'à ceux qu'on connait et on ne peut pas connaître tout le monde. Comme le dit le RFC, « " *Social interaction (beer) is a common thread amongst sharing partners to build trust relationships*" ».
— Par analogie avec les marques déposées, certains se sont demandés s'il faudrait un mécanisme de labelisation de la confiance.
— Plusieurs participants ont remarqué que le travail réel ne se faisait pas dans les structures officielles, mais dans des groupes fondés sur des relations de confiance. (Le RFC utilise le terme classique des geeks pour parler de ces groupes : "*cabals*".) Comme le dit le RFC pudiquement, « "*This was not disputed.*" » (autrement dit, tout le monde le savait bien mais ne le disait pas).

La section 4 du RFC concerne le « et maintenant ? ». Il y a eu un consensus sur la nécessité de la formation (au sens large). Par exemple, on trouve toujours des professionnels de l'Internet qui ne connaissent pas BCP 38 <https://www.bortzmeyer.org/bcp38.html>. Du travail pour les pédagogues (et les auteurs de blogs...)

Plus technique, la question des mécanismes techniques d'échange d'information a suscité des débats animés. Le RFC 6545 date de plus de dix ans. Il ne semble pas être universellement adopté, loin de là. Le groupe de travail DOTS <https://tools.ietf.org/wg/dots> fera-t-il mieux ? D'autres techniques ont été discutées comme TAXII <https://taxiiproject.github.io/> ou XMPP-Grid <https://www.ietf.org/proceedings/94/slides/slides-94-mile-7.pdf>. Ce dernier, fondé sur XMPP (RFC 6120) semble prometteur et est déjà largement mis en œuvre. Le groupe de travail nommé MILE <https://tools.ietf.org/wg/mile> a aussi un protocole nommé ROLIE (pas encore de RFC).