Les « Gamers » de la Sécu | La Mare du Gof

Le monde foisonnant de la sécu regroupe toutes sortes d'individualités, aux compétences diverses et multiples. Certains grands diplômés de cursus prestigieux, d'autres autodidactes remarqués -parfois employés dans le secteur, parfois amateurs œuvrant la nuit derrière leurs PC ; certains publient et se font lire, participent à des rassemblements professionnels et/ou passionnés, d'autres se font plus discrets et traitent directement avec les institutions et leurs représentants, les éditeurs, les Hacktivistes. D'audits facturés aux failles révélées, de papiers révélateurs aux vilains pistés et chassés, il y a toute une faune d'individus qui travaillent dans des domaines aux multiples compétences et exigences en raison de la sans cesse mouvance des technologies et des menaces. Néanmoins, il y a une catégorie toute particulière que je regarde avec de grands yeux et qui sont pour moi des extraterrestres : il s'agit de ce que j'appelle les « *Gamers* » de la sécu, les « teams » de CTF (« Capture The Flags »).

Il y a quelques semaines a eu lieu un cycle de conférences et d'ateliers à la Cantine à Paris, intitulé « Pas sage en Seine 2012 ». J'aime assez cette activité pour diverses raisons : elle est en langue française, elle est quasiment entièrement filmée, les vidéos sont rapidement disponibles à la suite de l'évènement (et téléchargeables), les « slides » aussi. Et la plupart des intervenants sont très disponibles et sympathiques, on peut sans peine les aborder sur le Net, que cela soit par IRC ou autres protocoles de messageries. La dominante de cette manifestation reste l'idéal de « neutralité » du Net, et les dénonciations des atteintes à celles-ci par divers procédés technologiques. Par delà cette grande thématique, on y trouve donc la façon de corriger ces atteintes, souvent le fait de « clusters » (groupes) d'initiative privée ; on y trouve également des débats sur les façons et les moyens de signaler ces atteintes (les différentes formes de journalisme numérique), les leviers juridiques et décisionnels possibles ou souhaités, les formes privées en local et en réseau pour s'en protéger, etc. Bref, des interventions de tous niveaux, toujours à mon sens intéressantes. Il y aurait matière à revenir longuement sur ce PSES pour en rapporter tous les éléments (si j'arrive à trouver le temps ^^).

En regardant le flux vidéo de cette manifestation, j'eus la surprise ainsi de voir évoquer les « CTF ». J'avais croisé le conférencier de temps à autre en IRC, et le suit sur Twitter. Il poste des éléments toujours très techniques et intéressants, et je le savais très impliqué dans les CTF avec une « team ». C'était la première fois que je voyais une de ses interventions ; les habitués de ces rassemblements (« CTF ») le connaissent certainement bien en revanche. Je l'ai écouté avec beaucoup de plaisir, la passion débordait de son intervention. J'évoquais la surprise quelques mots avant car, d'un œil extérieur, les intervenants me semblant plus sensibilisés aux grandes thématiques de neutralité, surveillance, liberté d'expression, free culture, etc., je les percevais surtout comme de grands spécialistes des réseaux, plutôt éloignés du strict aspect sécuritaire et technique associé aux « CTF ». C'est peut-être pour cela que sa présentation a brossé un portrait généraliste et plutôt informel de ce type d'épreuve, s'agissant plus de présenter et d'initier que de débattre avec un auditoire averti. Mais c'est finalement là tout l'intérêt de « PSES » que de proposer des interventions de tous niveaux sur toutes sortes de sujets, qui peuvent sembler assez éloignés au premier abord (mais finalement pas tant que ça, nous le verrons plus loin).

Il a commencé par aborder son intervention sur les éléments qui la motivaient (popularité grandissante de ce type de manifestations, beaucoup d'entreprises visibles montant leurs propres épreuves ; en marge de toutes les grandes conférences sécurité de haut niveau, vous trouverez toujours un « challenge/CTF » adossé à l'évènement ; il s'agit d'une démarche en équipe, permettant outre l'amusement de rester alerte sur toutes nouvelles vulnérabilités et méthodes de contournement). Pour lui, explique-t-il, professionnel de la sécurité, par delà l'amusement du jeu, il s'agit aussi d'une démarche

toute gagnante professionnellement. Il enchainait ensuite sur les origines du terme « CTF » et les analogies que l'on pouvait en faire avec les jeux vidéo (essentiellement), et les formes de participation que cela engendrait. Il insistait notamment sur la notion d'équipe où chacun apporte ses compétences au groupe (seul les épreuves d'équipe ont été abordées, même si on peut bien sûr s'y préparer en solo).

Il détaillait ensuite les modalités de participation à ce genre d'activités, et il y avait là des éléments qui ne m'étaient pas spontanément venus à l'esprit, comme notamment la nécessaire mise en relation des équipiers, via l'ouverture de canaux de communication dédiés (IRC, PAD, etc.), ou encore la veille relative aux évènements pour y glaner tout indice possible (avec les outils développés et alloués spécifiquement pour gagner du temps), les organisateurs en livrant malicieusement souvent en amont des épreuves, etc. Je n'avais pas du prêté attention à toute la logistique d'échange, de communication et de veille que les équipes mettent en place à l'approche d'un challenge, et qui serait sans doute la même dans le cadre d'un travail d'équipe journalistique, « forensique », en tous les cas d'investigations. Il y a là je crois un dénominateur commun notamment avec les grandes thématiques développés par l'idée de « PSES ». Enfin, il enchaînait en donnant des exemples d'épreuve pour donner une idée des challenges à résoudre, et finissait sur une liste de ressources francophones ou non pour suivre cette actualité et s'y former. Bref, un tour initiatique captivant de l'activité « CTF », avec toute l'ardeur du conférencier à en parler. Et si je les observe de loin avec de grands yeux et que je les crois venus d'ailleurs, c'est que leurs mises en œuvre collectives de connaissances diversement assimilées, avec les affinités et intuitions de chacun, permet des réalisations et des résolutions impressionnantes.

A ceux qui pourraient se demander à quoi cela sert, j'aurais tendance, de l'extérieur, à croire que cela doit insuffler méthodologie, curiosité, acuité à trouver l'élément faillible de concert avec ses partenaires, à affûter les réflexes et les techniques face un problème donné ; des qualités précieuses finalement dans toutes sortes de domaines de compétences. Aux professionnels de confirmer ce que cela leur apporte, au-delà du strict jeu, de la publicité inhérente aux évènements associés et de la renommée suite aux prouesses réalisées. La technicité requise et démontrée reste en tous les cas impressionnante et traduit très certainement un investissement personnel de chacun entier et sans aucun doute très envahissant, comme le sont toutes les passions. Les épreuves « CTF » ne sont-elles pas finalement des vitrines de compétences et de formidables trouveuses (parce qu'elles les révèlent) et couveuses (parce qu'elles les entretiennent) de talents ?

- *Les diapositives de cette intervention en français : http://6dev.net/talk/pses-2012/pses_ctf_debriefings_fr.pdf*
- *Même diapositives, en version anglaise : http://6dev.net/talk/pses-2012/pses_ctf_debriefings_en.pdf*
- *La vidéo : http://lacantine.ubicast.eu/videos/17-06-2012-163059/*